ΘΕΩΡΙΑ
ΑΡΙΘΜΩΝ

Πρόλογος

Το παρόν βιβλίο αποτελεί ένα ακόμη βήμα της Ελληνικής Μαθηματικής Εταιρείας στη συνεχή προσπάθειά της για αναβάθμιση της Μαθηματικής Παιδείας στη χώρα μας, για την υποστήριξη του έργου των μαθηματικών, αλλά και για την υποβοήθηση της μελέτης των μαθητών και σπουδαστών.

Ο κύριος στόχος του βιβλίου είναι η απόδοση μιας εισαγωγικής, αλλά όσο το δυνατόν πληρέστερης, παρουσίασης της Θεωρίας των Αριθμών, ενός από τους βασικότερους και πολύ ελκυστικούς κλάδους των Μαθηματικών.

Το Διοικητικό Συμβούλιο της Ελληνικής Μαθηματικής Εταιρείας εκφράζει τις θερμές ευχαριστίες τους προς

(α) τους συγγραφείς του βιβλίου:

Βλάμο Παναγιώτη, Διδάκτορα Μαθηματικών Ε. Μ. Πολυτεχνείου,
Ράππο Ευστράτιο, Πτυχιούχο Μαθηματικών Παν/μίου Cambridge,
Ψαρράκο Παναγιώτη, Διδάκτορα Μαθηματικών Ε. Μ. Πολυτεχνείου,

οι οποίοι κατέβαλαν φιλότιμη μακροχρόνια προσπάθεια για τη συγγραφή και την επιμελημένη παρουσίαση του βιβλίου.

(β) τους κριτές του βιβλίου:

Δημάκο Γεώργιο, Λέκτορα Πανεπιστημίου Αθηνών,
Φελούρη Ανάργυρο, Επίκ. Καθηγητή Ε. Μ. Πολυτεχνείου,

για τις προσπάθειες που κατέβαλλαν για τη βελτιωμένη παρουσίαση του βιβλίου.

(γ) τους υπαλλήλους της Ε.Μ.Ε. Λαμπρινή Σταθονίκου και Κώστα Στάικο για την επιμελημένη δακτυλογράφηση του βιβλίου.

Το Διοικητικό Συμβούλιο της Ε.Μ.Ε.

Περιεχόμενα

1 Διαιρετότητα **1**

1.1 Ευκλείδεια Διαίρεση 1
1.2 Διαιρετότητα 12
1.3 Μέγιστος Κοινός Διαιρέτης 22
1.4 Γραμμική Διοφαντική Εξίσωση 36
1.5 Ελάχιστο Κοινό Πολλαπλάσιο 45
1.6 Πρώτοι Αριθμοί 51
1.7 Πλήθος και Άθροισμα Διαιρετών 64

2 Αλγεβρικές Ισοτιμίες **77**

2.1 Ορισμοί-Ιδιότητες 77
2.2 Η γραμμική ισοτιμία $ax \equiv \beta\,(mod\nu)$ 88
2.3 Η συνάρτηση φ του Euler 96
2.4 Τα Θεωρήματα Fermat και Euler 104
2.5 Το Θεώρημα Wilson 111
2.6 Εφαρμογές των Ισοτιμιών 113
2.6.1 Κριτήρια Διαιρετότητας 113
2.6.2 Η ημέρα της εβδομάδας 114

3 Ισοτιμίες Ανώτερου Βαθμού **123**

3.1 Τετραγωνικά Κατάλοιπα 123
3.2 Ο Συμβολισμός του Legendre 131
3.3 Γενική μορφή λύσης ισοτιμίας δευτέρου βαθμού 140

4 Η εξέλιξη της Θεωρίας των Αριθμών **151**

4.1 Εισαγωγή 151
4.2 Η κατανομή των πρώτων 153

4.2.1 Το Θεώρημα των Πρώτων Αριθμών 154
4.2.2 Τα κενά ανάμεσα στους πρώτους 155
4.2.3 Πρώτοι σε αριθμητικές προόδους 157
4.3 Η μέθοδος των Hardy-Littlewood 158
4.3.1 Η συνάρτηση διαμέρισης p(ν). 158
4.3.2 Το πρόβλημα του Goldbach 161
4.3.3 Το πρόβλημα του Waring 162
4.4 Η Μέθοδος του Κόσκινου 164
4.5 Προσεγγιστικές μέθοδοι, Διοφαντικές εξισώσεις και υπερβατικοί αριθμοί 166
4.5.1 Προσεγγίσεις αρρήτων με ρητούς 166
4.5.2 Διοφαντικές εξισώσεις 168
4.5.3 Υπερβατικοί αριθμοί 168
4.5.4 Σχετικά Αποτελέσματα 169
4.6 Αριθμητικές συναρτήσεις και εκτιμήσεις εκθετικών αθροισμάτων 170
4.7 Υπολογιστική Θεωρία Αριθμών 172
4.8 Το μεγάλο Θεώρημα του Fermat 180
Λύσεις των Ασκήσεων 183
Βιβλιογραφία 259
Ευρετήριο Όρων 263

Κεφάλαιο 1

Διαιρετότητα

Αντί Εισαγωγής

Μονὰς ἐστίν, καθ' ἣν ἕκαστον τῶν ὄντων ἓν λέγεται.
Ἀριθμὸς δέ τὸ ἐκ μονάδων συγκείμενον πλῆθος.

(Στοιχεία Ευκλείδη, Βιβλίο VII)

God created the integers, all else is the work of man.
Ο Θεός δημιούργησε τους ακεραίους, τα υπόλοιπα είναι έργα των ανθρώπων.

(Leopold Kronecker)

1.1 Ευκλείδεια Διαίρεση

Η έννοια της διαίρεσης είναι στενά συνδεδεμένη με την πράξη της πρόσθεσης και μάλιστα με το πρόβλημα της εύρεσης της καλύτερης προσέγγισης ενός φυσικού αριθμού α από τον φυσικό β, με $\alpha > \beta$. Για τον λόγο αυτό θεωρούμε την ακολουθία

$$\alpha, \alpha - \beta, \alpha - 2\beta, \alpha - 3\beta, \ldots$$

Προφανώς η καλύτερη προσέγγιση επιτυγχάνεται, όταν η διαφορά $\alpha - \nu\beta$ είναι θετική και γίνει η μικρότερη δυνατή. Η τιμή του ν για την οποία συμβαίνει αυτό ονομάζεται **πηλίκο** της διαίρεσης α δια β και ο αριθμός $\upsilon = \alpha - \nu\beta$ **υπόλοιπο**.

Έτσι κάθε φυσικός αριθμός α γράφεται στην μορφή:

$$\alpha = \pi\beta + \upsilon,$$

όπου $\pi \geq 0$ είναι το πηλίκο και $0 \leq \upsilon < \beta$ είναι το υπόλοιπο. Το υπόλοιπο είναι πάντα αυστηρά μικρότερο του β αφού διαφορετικά η διαφορά $\alpha - (\pi + 1)\beta$ θα ήταν η καλύτερη προσέγγιση.
Οι αριθμοί π και υ είναι μοναδικοί, αφού αν υποθέσουμε ότι υπάρχουν δύο άλλοι ακέραιοι π' και υ' τέτοιοι ώστε $\alpha = \pi'\beta + \upsilon'$ με $0 \leq \upsilon' < \beta$, $\pi \geq 0$ και $\upsilon > \upsilon'$, τότε $0 < \upsilon - \upsilon' = (\pi - \pi')\beta$. Επειδή ο $\pi' - \pi$ είναι ακέραιος, αν $\pi' \neq \pi$ θα έχουμε $(\pi' - \pi)\beta \geq \beta$, δηλαδή $\upsilon - \upsilon' \geq \beta$ αδύνατο, αφού $\upsilon < \beta$. Άρα $\pi = \pi'$ και $\upsilon = \upsilon'$.
Τα προηγούμενα συμπεράσματα μας οδηγούν στο γνωστό **Αλγόριθμο της διαίρεσης φυσικών αριθμών του Ευκλείδη:**

Θεώρημα 1.1.1 (Ευκλείδης)
Αν α και β είναι δύο φυσικοί αριθμοί με $\alpha > \beta$, τότε μπορούμε να βρούμε μοναδικούς ακέραιους αριθμούς π και υ με $\pi \geq 0$, $\upsilon \geq 0$ τέτοιους ώστε :

$$\alpha = \pi\beta + \upsilon, \text{ όπου } \upsilon < \beta.$$

Ο αλγόριθμος της διαίρεσης που περιγράψαμε προηγουμένως μπορεί να γενικευθεί και στην περίπτωση όπου οι α, β είναι ακέραιοι, με $0 \leq \upsilon < |\beta|$.
Οι αριθμοί α, β όπως τους ορίσαμε παραπάνω ονομάζονται **διαιρετέος** και **διαιρέτης** αντίστοιχα.
Αν ισχύει $\upsilon = 0$ τότε λέμε ότι ο αριθμός β **διαιρεί** τον α.
Αν δύο ακέραιοι αριθμοί αφήνουν το ίδιο υπόλοιπο διαιρούμενοι με έναν κοινό διαιρέτη τότε ονομάζονται **ισοϋπόλοιποι** ως προς τον κοινό τους διαιρέτη.

Ιδιαίτερο ενδιαφέρον παρουσιάζει η διαίρεση ενός ακεραίου αριθμού με τον 2. Τότε προκύπτουν δύο περιπτώσεις :

(i) Να έχουμε υπόλοιπο $\upsilon = 0$, οπότε ο α γράφεται στη μορφή $\alpha = 2\kappa$ για κάποιον ακέραιο κ, και λέγεται **άρτιος**.
(ii) Να έχουμε υπόλοιπο $\upsilon = 1$, οπότε ο α γράφεται στη μορφή $\alpha = 2\kappa+1$ για κάποιον ακέραιο κ, και λέγεται **περιττός**.

Εύκολα μπορεί να συμπεράνει κανείς πως το άθροισμα δύο αρτίων ή δύο περιττών είναι άρτιος, το άθροισμα άρτιου με περιττό είναι περιττός, το γινόμενο δύο άρτιων ή άρτιου με περιττό είναι άρτιος και το γινόμενο δύο περιττών είναι περιττός. Για παράδειγμα, αν $\alpha = 2\kappa + 1$ και $\beta = 2\lambda + 1$, τότε $\alpha + \beta = 2(\kappa + \lambda + 1)$ είναι άρτιος.

Αν εξετάσουμε τη διαίρεση ενός φυσικού ν με τον 3 τότε διαπιστώνουμε ότι κάθε ακέραιος α γράφεται σε μία από τις τρεις μορφές:

$$\alpha = 3\kappa\,,\ \alpha = 3\kappa + 1\,,\ \alpha = 3\kappa + 2,\ \kappa \in \mathbf{Z}$$

ανάλογα με το αν το υπόλοιπο της διαίρεσης του α με το 3 είναι 0, 1 ή 2 αντίστοιχα. Γενικότερα, αν χρησιμοποιήσουμε για διαιρέτη έναν φυσικό κ, τότε κάθε ακέραιος α γράφεται στη μορφή

$$\alpha = \pi\kappa + \upsilon$$

όπου $\upsilon = 0$ ή 1 ή $2 \ldots$ ή $\kappa - 1$.

Με τον τρόπο αυτό πετυχαίνουμε μια *διαμέριση* του συνόλου των ακεραίων αριθμών σε κ υποσύνολα[1]:

$$Z_0 = \{\pi\kappa/\pi = 0, \pm 1, \pm 2, \ldots\}$$

$$Z_1 = \{\pi\kappa + 1/\pi = 0, \pm 1 \pm 2, \ldots\}$$

$$\vdots$$

$$Z_{\kappa-1} = \{\pi\kappa + \kappa - 1/\pi = 0, \pm 1, \pm 2, \ldots\}\,.$$

Η σημασία της διαμέρισης του $\mathbf{Z}$ σε κλάσεις οφείλεται στο ότι στοιχεία της ίδιας κλάσης έχουν παρόμοια συμπεριφορά ως προς τη διαίρεση. Έτσι, αντί να μελετήσουμε τη συμπεριφορά των ακεραίων ως προς κάποια ιδιότητα μπορούμε να εξετάσουμε τη συμπεριφορά των κλάσεων, το πλήθος των οποίων είναι πεπερασμένο.

---

[1] Τα υποσύνολα αυτά αποτελούν "κλάσεις ισοδυναμίας", αφού μπορούμε για ακέραιους x, y να ορίσουμε τη σχέση $x \sim y$ αν και μόνο αν οι x και y αφήνουν το ίδιο υπόλοιπο αν διαιρεθούν με τον κ. Η σχέση $\sim$ είναι σχέση ισοδυναμίας επειδή $x \sim x$, $x \sim y \Longleftrightarrow y \sim x$, $x \sim y$ και $y \sim z \Longrightarrow x \sim z$ για κάθε x, y, z ακέραιους. Η κάθε κλάση περιέχει τους αριθμούς που είναι ισοδύναμοι μεταξύ τους και μόνον αυτούς.

Παράδειγμα
Να αποδείξετε ότι ανάμεσα σε τρεις διαδοχικούς ακεραίους ένας ακριβώς από αυτούς αφήνει υπόλοιπο 1 διαιρούμενος με το 3.
Απόδειξη
Έστω ν, $\nu+1$, $\nu+2$ οι τρεις διαδοχικοί ακέραιοι αριθμοί.
(i) Αν $\nu=3\kappa$, τότε $\nu+1=3\kappa+1$ και $\nu+2=3\kappa+2$.
(ii)Αν $\nu=3\kappa+1$, τότε $\nu+1=3\kappa+2$ και $\nu+2=3\kappa+3=3(\kappa+1)$.
(iii)Αν $\nu=3\kappa+2$, τότε $\nu+1=3\kappa+3=3(\kappa+1)$ και $\nu+2=3\kappa+4=3(\kappa+1)+1$.

Σε κάθε περίπτωση υπάρχει ένας μόνο αριθμός της μορφής $3\lambda+1$, ο οποίος αφήνει υπόλοιπο 1 διαιρούμενος με το 3.

Ένα κριτήριο προσδιορισμού ισοϋπόλοιπων αριθμών αποτελεί το ακόλουθο θεώρημα.

Θεώρημα 1.1.2
Δύο ακέραιοι αριθμοί είναι ισοϋπόλοιποι ως προς τον ακέραιο $\beta \neq 0$ αν και μόνο αν ο β διαιρεί τη διαφορά τους.

Απόδειξη
Έστω $\alpha_1 = \pi_1\beta + \upsilon_1$ και $\alpha_2 = \pi_2\beta + \upsilon_2$ με $0 \leq \upsilon_1 < |\beta|$ και $0 \leq \upsilon_2 < |\beta|$. Αν $\upsilon_1 = \upsilon_2$, τότε αφαιρώντας τις παραπάνω σχέσεις κατά μέλη έχουμε $\alpha_1 - \alpha_2 = (\pi_1 - \pi_2)\beta$, οπότε, ο ακέραιος αριθμός β διαιρεί τον $\alpha_1 - \alpha_2$. Αντίστροφα, αν $\alpha_1 - \alpha_2 = \pi\beta$, τότε $\alpha_1 - (\pi_2\beta + \upsilon_2) = \pi\beta$ και $\alpha_1 = (\pi + \pi_2)\beta + \upsilon_2$.

Το επόμενο θεώρημα εκφράζει πράξεις που καταλήγουν σε ισοϋπόλοιπους αριθμούς.

Θεώρημα 1.1.3
Για οποιουσδήποτε ν ακέραιους αριθμούς, το άθροισμά τους και το άθροισμα των υπολοίπων τους διαιρούμενων με έναν κοινό διαιρέτη είναι ισοϋπόλοιποι αριθμοί ως προς τον διαιρέτη αυτό. Επίσης το ίδιο ισχύει για το γινόμενό τους και το γινόμενο των υπολοίπων τους.

Απόδειξη
Έστω $\alpha_i = \pi_i\beta + \upsilon_i$ οι ν ακέραιοι, όπου β ο κοινός διαιρέτης και υ_i τα

υπόλοιπα, με $1 \leq i \leq \nu$. Τότε έχουμε ότι:

$$(\alpha_1 + \alpha_2 + \ldots + \alpha_\nu) - (\upsilon_1 + \upsilon_2 + \ldots + \upsilon_\nu) = (\pi_1 + \pi_2 + \ldots + \pi_\nu)\beta,$$

δηλαδή ο β διαιρεί τη διαφορά του αριστερού μέλους, οπότε οι αριθμοί $\alpha_1 + \alpha_2 + \ldots + \alpha_\nu$ και $\upsilon_1 + \upsilon_2 + \ldots + \upsilon_\nu$ είναι ισοϋπόλοιποι.
Όμοια έχουμε ότι $\alpha_1\alpha_2 \cdots \alpha_\nu = (\pi_1\beta + \upsilon_1)(\pi_2\beta + \upsilon_2) \cdots (\pi_\nu\beta + \upsilon_\nu)$ και παρατηρούμε ότι όλοι οι όροι του δεξιού μέλους έχουν παράγοντα το β εκτός από ένα, οπότε $\alpha_1\alpha_2 \cdots \alpha_\nu - \upsilon_1\upsilon_2 \cdots \upsilon_\nu = A\beta$, όπου A ένας ακέραιος, οπότε οι αριθμοί $\alpha_1\alpha_2 \cdots \alpha_\nu$ και $\upsilon_1\upsilon_2 \cdots \upsilon_\nu$ είναι ισοϋπόλοιποι.

Εφαρμογές 1.1

1. Αν ο α είναι ένας φυσικός αριθμός και β το τελευταίο ψηφίο του τότε οι α και β διαιρούμενοι με γ=2 ή 5 ή 10, είναι ισοϋπόλοιποι.

   Απόδειξη.
   Η διαφορά $\alpha - \beta$ τελειώνει σε μηδέν, οπότε οι αριθμοί 2, 5 και 10 διαιρούν τη διαφορά $\alpha - \beta$ και η απόδειξη είναι άμεση από το Θεώρημα 1.1.2

2. Αν α είναι ένας φυσικός αριθμός και β είναι ο διψήφιος φυσικός που σχηματίζουν τα δύο τελευταία ψηφία του α, τότε οι α και β διαιρούμενοι με τον γ=4 ή 20 ή 25 ή 50 ή 100, είναι ισοϋπόλοιποι.

   Απόδειξη.
   Προφανής, αφού οι αριθμοί 4, 20, 25, 50, 100 διαιρούν την διαφορά $\alpha - \beta$.

3. Να βρείτε το υπόλοιπο της διαίρεσης $(451^{41} \cdot 7707^{21} : 8)$.

   Λύση.
   Οι αριθμοί 451 και 7707 διαιρούμενοι με τον 8 αφήνουν υπόλοιπο 3. Από το Θεώρημα 1.1.3 η διαίρεση $(451^{41} \cdot 7707^{21} : 8)$ αφήνει το ίδιο υπόλοιπο με την διαίρεση $(3^{41} \cdot 3^{21} : 8)$ ή την $(9^{31} : 8)$. Άρα το υπόλοιπο της διαίρεσης είναι 1.

4. Να βρείτε τα δυνατά υπόλοιπα της διαίρεσης του τετραγώνου ενός οποιουδήποτε ακεραίου με το 4.

   Λύση.
   Αν ο ακέραιος α είναι άρτιος, δηλαδή α=2ν, τότε $\alpha^2 = 4\nu^2$.
   Αν ο α είναι περιττός, δηλαδή $\alpha = 2\nu+1$, τότε $\alpha^2 = 4\nu^2+4\nu+1 = 4(\nu^2+\nu)+1$. Άρα το ζητούμενο υπόλοιπο είναι 0 ή 1.

5. Να βρείτε τα δυνατά υπόλοιπα της διαίρεσης του τετραγώνου ενός περιττού ακεραίου με το 8.

   Λύση.
   Αν $\nu = 2\kappa + 1$ ένας περιττός τότε έχουμε:

$\nu^2 = (2x+1)^2 = 4x^2+4x+1 = 4x(x+1)+1$. Οι αριθμοί x και $x+1$ ως διαδοχικοί ακέραιοι θα είναι ο ένας άρτιος και ο άλλος περιττός. Άρα το γινόμενό τους είναι άρτιος και γράφεται ως $x(x+1) = 2\lambda$. Έτσι $\nu^2 = 8\lambda + 1$ οπότε το ζητούμενο υπόλοιπο είναι πάντα το 1.
Συμπερασματικά: Κάθε τέλειο τετράγωνο είναι της μορφής $8x$, $8x+1$ ή $8x+4$.

6. Να αποδείξετε ότι κανένας από τους αριθμούς 11, 111, 1111, ... δεν είναι τέλειο τετράγωνο ακεραίου.

   Απόδειξη.
   Ο αριθμός 11 καταρχήν δεν είναι τέλειο τετράγωνο ακεραίου. Ένας τυχαίος αριθμός της μορφής $111\ldots111$ μεγαλύτερος του 11 μπορεί να γραφεί ως εξής:

$$111\ldots111 = 111\ldots108 + 3.$$

   Όμως ο αριθμός $111\ldots108$ είναι πολλαπλάσιο του 4. Άρα ο $111\ldots111$ είναι της μορφής $4x+3$ οπότε αποκλείεται να είναι τέλειο τετράγωνο κάποιου ακεραίου, σύμφωνα με την Εφαρμογή 5.

7. Να βρείτε τους φυσικούς αριθμούς ν και μ που ικανοποιούν τη σχέση :

$$\frac{1}{\nu} + \frac{\nu}{\mu} + \frac{1}{\nu\mu} = 1.$$

   Λύση.
   Πολλαπλασιάζοντας τη σχέση $\frac{1}{\nu} + \frac{\nu}{\mu} + \frac{1}{\nu\mu} = 1$ με $\mu\nu$ έχουμε

$$\mu + \nu^2 + 1 = \mu\nu \text{ ή } \mu\nu - \mu = \nu^2 + 1 \text{ ή } (\nu-1)\mu = \nu^2 + 1.$$

   Αν είναι $\nu = 1$, τότε προκύπτει $0=2$, αδύνατο. Άρα πρέπει $\nu \neq 1$ και

$$\mu = \frac{\nu^2+1}{\nu-1} = \frac{(\nu-1)^2+2}{\nu-1} = \nu + 1 + \frac{2}{\nu-1}.$$

   Εφόσον οι μ και ν είναι φυσικοί αριθμοί, οι μοναδικές τιμές που μπορεί να λάβει ο $\nu-1$ είναι 1 ή 2. Άρα οι ζητούμενες λύσεις είναι $(\mu,\nu) = (5,2)$ ή $(\mu,\nu) = (5,3)$.

8. Αν για έναν φυσικό κ θεωρήσουμε τον $\nu = \kappa^2 + 1$ να αποδειχθεί ότι ο ν^2 δεν είναι της ίδιας μορφής.

Απόδειξη.
Ας υποθέσουμε ότι υπάρχει φυσικός λ τέτοιος ώστε $\nu = \kappa^2 + 1$ και $\nu^2 = \lambda^2 + 1$. Τότε:

$$\begin{aligned} \lambda^2 + 1 &= (\kappa^2 + 1)^2 \quad \text{ή} \\ \lambda^2 &= \kappa^2(\kappa^2 + 2) \quad \text{ή} \\ \left(\tfrac{\lambda}{\kappa}\right)^2 &= \kappa^2 + 2. \end{aligned}$$

Άρα ο λ/κ είναι φυσικός και έστω $\lambda/\kappa = \rho$. Έχουμε λοιπόν $\rho^2 = \kappa^2 + 2$, το οποίο είναι αδύνατο, αφού $\kappa^2 = 4\mu$ ή $\kappa^2 = 4\mu + 1$, οπότε $\kappa^2 + 2 = 4\mu + 2$ ή $\kappa^2 + 2 = 4\mu + 3$.
Επομένως, ο ν δεν μπορεί να είναι τέλειο τετράγωνο ακεραίου.
Άρα δεν υπάρχει φυσικός ν, τέτοιος ώστε οι ν και ν^2 να είναι της μορφής $\kappa^2 + 1$.

9. Να αποδειχθεί ότι καμμία δύναμη του 2 δεν γράφεται ως άθροισμα κ διαδοχικών φυσικών ($\kappa > 1$) .

Απόδειξη.
Ας υποθέσουμε ότι υπάρχουν κ διαδοχικοί φυσικοί $\mu, \mu + 1, \mu + 2, \ldots, \mu + \kappa - 1$ με $\mu > 0$, τέτοιοι ώστε

$$\mu + (\mu + 1) + \ldots + (\mu + \kappa - 1) = 2^\nu$$

για κατάλληλο φυσικό ν.
Επομένως $2^\nu = \kappa\mu + (1 + 2 + \ldots + \kappa - 1) = \kappa\mu + \frac{(\kappa-1)\kappa}{2}$ και $2^{\nu+1} = 2\kappa\mu + (\kappa - 1)\kappa = \kappa(2\mu + \kappa - 1)$.
Για $\kappa = 0$, προκύπτει $0 = 2^{\nu+1}$, αδύνατο. Για $\kappa \neq 0$, το αριστερό μέλος της ισότητας είναι γινόμενο δύο άρτιων ακεραίων, ενώ το δεξί μέλος της ισότητας είναι γινόμενο άρτιος και περιττού ακεραίου, άτοπο. Επομένως καμία δύναμη του 2 δεν γράφεται ως άθροισμα κ διαδοχικών φυσικών.

Ασκήσεις 1.1

Α' Ομάδα

1. Να υπολογισθούν το πηλίκο και το υπόλοιπο της διαίρεσης των παρακάτω αριθμών με τον 17.
   (i) 100 (ii) -100 (iii) 289 (iv) -342

2. Να αποδειχθεί ότι το γινόμενο δύο ακεραίων είναι περιττός ακέραιος αν και μόνο αν οι δύο ακέραιοι είναι περιττοί.

3. Να αποδειχθεί ότι:
   (i) Το γινόμενο κ φυσικών $\alpha_1, \alpha_2, \ldots, \alpha_\kappa$ είναι περιττός αριθμός αν και μόνο αν όλοι τους είναι περιττοί.
   (ii)Η δύναμη ενός φυσικού α είναι περιττός αριθμός αν και μόνο αν ο α είναι περιττός.

4. Να αποδειχθεί ότι:
   (i) το γινόμενο δύο ακεραίων της μορφής $4\kappa + 1$ είναι επίσης της ίδιας μορφής,
   (ii) το γινόμενο δύο ακεραίων της μορφής $4\kappa + 3$ είναι της μορφής $4\kappa + 1$,
   (iii)το γινόμενο δύο ακεραίων της μορφής $6\kappa + 5$ είναι της μορφής $6\kappa + 1$.

5. Να αποδειχθεί ότι κάθε ακέραιος της μορφής $6\kappa + 5$ είναι επίσης της μορφής $3\kappa - 1$. Ισχύει το αντίστροφο;

6. Να αποδειχθεί ότι κάθε φυσικός αριθμός της μορφής $8\kappa + 5$ γράφεται στη μορφή $4\lambda + 1$. Ισχύει το αντίστροφο;

7. Αν ένας ακέραιος α διαιρούμενος με τον $\beta = 16$ αφήνει υπόλοιπο $\upsilon = 11$, βρείτε το υπόλοιπο της διαίρεσης του $\alpha + \kappa$ δια β, για κ=1, 3, 5, 7, 9, 105, -7.

8. Να αποδειχθεί ότι το τετράγωνο κάθε φυσικού της μορφής $\nu = 5\kappa + 1$ είναι της ίδιας μορφής.

9. Να αποδείξετε ότι το τετράγωνο κάθε ακέραιου είναι της μορφής 3κ ή $3\kappa + 1$.

10. Να αποδειχθεί ότι για κάθε φυσικό ν ο αριθμός $3\nu^2 - 1$ δεν μπορεί να γραφεί ως τέλειο τετράγωνο ακεραίου.

11. Να αποδειχθεί ότι κανένα τετράγωνο ακεραίου αριθμού δεν είναι της μορφής $5\kappa + 2$ ή $5\kappa + 3$.

Β' Ομάδα

12. Να αποδειχθεί ότι για κάθε τριάδα ακεραίων α, β, γ το γινόμενο $N = (\alpha - \beta)(\beta - \gamma)(\gamma - \alpha)$ είναι άρτιος αριθμός.

13. Να αποδείξετε ότι το άθροισμα των τετραγώνων δύο περιττών ακεραίων δεν είναι ποτέ τέλειο τετράγωνο ακεραίου ή ισοδύναμα ότι δεν υπάρχει ορθογώνιο τρίγωνο του οποίου οι δύο κάθετες πλευρές είναι περιττοί φυσικοί και η υποτείνουσα φυσικός αριθμός.

14. Να αποδείξετε ότι ο κύβος κάθε ακεραίου είναι της μορφής 9κ, $9\kappa+1$ ή $9\kappa+8$.

15. Να αποδείξετε ότι η διαφορά των κύβων δύο διαδοχικών ακεραίων είναι πάντα περιττός αριθμός.

16. Να αποδείξετε ότι αν ένας ακέραιος αριθμός α είναι ταυτόχρονα τετράγωνο και κύβος κάποιων ακεραίων, τότε θα είναι της μορφής $\alpha = 7\kappa$ ή $\alpha = 7\kappa + 1$ (για παράδειγμα: $64 = 8^2 = 4^3 = 7 \cdot 9 + 1$).

17. Να αποδειχθεί ότι για κάθε περιττό ακέραιο α, ο α^4 είναι της μορφής $16\mu + 1$.

18. Να αποδειχθεί ότι η εξίσωση $x^2 + y^2 = 1999$ δεν έχει ακέραιες λύσεις.

19. Έστω ένας περιττός ακέραιος α και ένας άρτιος φυσικός ν. Να αποδειχθεί ότι η εξίσωση

$$x^\nu + x^{\nu-1} + \ldots + x^2 + x + \alpha = 0$$

δεν έχει ακέραιες ρίζες.

20. Να αποδειχθεί ότι το τελευταίο ψηφίο του τετραγώνου κάθε ακεραίου είναι ένας από τους αριθμούς 0, 1, 4, 5, 6, 9.

1.2 Διαιρετότητα

Στην προηγούμενη παράγραφο διαμερίσαμε τους ακεραίους σε κλάσεις ισοϋπολοίπων ως προς κάποιον δοσμένο διαιρέτη. Θα μελετήσουμε κατόπιν την κλάση ισοϋπολοίπων $\mathbf{Z}_0$, δηλαδή το σύνολο των ακεραίων που αφήνουν υπόλοιπο 0 ως προς την διαίρεση με έναν δοσμένο αριθμό.
Εστω δύο ακέραιοι αριθμοί α και β με $\beta \neq 0$. Ο αριθμός α καλείται **πολλαπλάσιο** του β ή ισοδύναμα ο β είναι **παράγοντας** του α αν και μόνο αν η διαίρεση α διά β αφήνει υπόλοιπο μηδέν, οπότε γράφουμε $\beta \mid \alpha$.

Θεώρημα 1.2.1
Για οποιουσδήποτε ακέραιους αριθμούς α, β, γ και δ ισχύουν :
(i) Αν $\alpha \mid \beta$ και $\beta \mid \alpha$, τότε $\alpha = \pm\beta$, όπου $\alpha, \beta \neq 0$.
(ii) Αν $\alpha \mid \beta$ και $\beta \mid \gamma$, τότε $\alpha \mid \gamma$, όπου $\alpha, \beta \neq 0$.
(iii) Αν $\alpha \mid \beta$, τότε $\alpha \mid \lambda\beta$ για κάθε ακέραιο $\lambda \neq 0$, όπου $\alpha \neq 0$.
(iv) Αν $\alpha\beta \mid \gamma$, τότε $\alpha \mid \gamma$ και $\beta \mid \gamma$, όπου $\alpha, \beta \neq 0$.
(v) Αν $\alpha \mid \beta$, τότε $\alpha\gamma \mid \beta\gamma$, όπου $\alpha, \gamma \neq 0$.
(vi) Αν $\alpha \mid \beta$ και $\gamma \mid \delta$, τότε $\alpha\gamma \mid \beta\delta$, όπου $\alpha, \gamma \neq 0$.
(vii) Αν $\alpha \mid \beta$, τότε $|\alpha| \leq |\beta|$, όπου $\alpha, \beta \neq 0$.
(viii) Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$, τότε $\alpha \mid (x\beta + y\gamma)$, για κάθε ζεύγος ακεραίων x και y, όπου $\alpha \neq 0$.
(ix) Αν $\alpha \mid (\beta + \gamma)$ και $\alpha \mid \beta$, τότε $\alpha \mid \gamma$, όπου $\alpha \neq 0$.
(x) $(-1) \mid \alpha$ και $1 \mid \alpha$, οι οποίοι ονομάζονται **τετριμμένοι** παράγοντες του α.

Απόδειξη.
Οι σχέσεις (i)-(x) προκύπτουν άμεσα από τον ορισμό.

Κριτήρια Διαιρετότητας

Η κατάταξη των ακεραίων αριθμών σε κλάσεις ισοϋπολοίπων είναι άμεσα συνδεδεμένη με το πρόβλημα εύρεσης υπολοίπου. Για το λόγο αυτό και είναι αναγκαία τα κριτήρια που ακολουθούν.

Πρόταση 1.2.2
Αν α είναι ένας φυσικός αριθμός και β είναι το άθροισμα των ψηφίων του α, τότε οι α και β διαιρούμενοι με γ=3 ή 9 είναι ισοϋπόλοιποι. Δηλαδή,

ένας φυσικός αριθμός και το άθροισμα των ψηφίων του, αφήνουν το ίδιο υπόλοιπο διαιρούμενοι με 3 ή 9.

Απόδειξη.

Έστω β το άθροισμα των ψηφίων του α και γ=3 ή γ=9. Αν $\alpha_0, \alpha_1, \ldots, \alpha_x$ είναι τα ψηφία του α και $\alpha = \alpha_x 10^x + \ldots + \alpha_1 10 + \alpha_0$, τότε

$$\alpha = (\alpha_x + \ldots + \alpha_1 + \alpha_0) + (\alpha_x \cdot \overbrace{99\ldots9}^{x-\text{φορές}} + \ldots + \alpha_1 \cdot 9) = \beta + 9\lambda$$

όπου $\lambda = \alpha_x \cdot \overbrace{11\ldots1}^{x-\text{φορές}} + \ldots + \alpha_1$.
Επομένως οι αριθμοί 3 και 9 διαιρούν τη διαφορά $\alpha - \beta$ και από την Πρόταση 1.1.2 η απόδειξη ολοκληρώθηκε.

Αν σε έναν φυσικό αριθμό ν αριθμήσουμε τα ψηφία του από δεξιά προς τα αριστερά ξεκινώντας από την θέση 1, τότε τα ψηφία του α που βρίσκονται σε άρτια (αντίστοιχα περιττή) θέση ονομάζονται *ψηφία άρτιας* (αντίστοιχα **περιττής**) **τάξης**. Έτσι, π.χ., στον α=128 τα ψηφία 1 και 8 είναι τα ψηφία περιττής τάξης.

Πρόταση 1.2.3
Έστω α είναι ένας φυσικός αριθμός, σ_1 το άθροισμα των ψηφίων περιττής τάξης και σ_2 το άθροισμα των ψηφίων άρτιας τάξης του α. Οι αριθμοί α και $\sigma_1 - \sigma_2$ διαιρούμενοι με τον 11 είναι ισοϋπόλοιποι.

Απόδειξη.

Αν ο φυσικός α είναι της μορφής $\alpha = \alpha_x 10^x + \ldots + \alpha_1 10 + \alpha_0$, τότε γράφεται:

$$\begin{aligned} \alpha &= \alpha_0 + \alpha_1(11-1) + \alpha_2(99+1) + \alpha_3(1001-1) + \ldots = \\ &= (\alpha_0 - \alpha_1 + \alpha_2 - \alpha_3 + \ldots) + \alpha_1 11 + \alpha_2 99 + \alpha_3 1001 + \ldots = \\ &= \sigma_1 - \sigma_2 + 11(\alpha_1 + \alpha_2 9 + \alpha_3 91 + \ldots) \end{aligned}$$

Επομένως, ο αριθμός 11 διαιρεί την διαφορά $\alpha - (\sigma_1 - \sigma_2)$ και η απόδειξη ολοκληρώθηκε.

Συνοψίζοντας, έχουμε τα ακόλουθα κριτήρια διαιρετότητας:

Έστω α ένας φυσικός αριθμός.

1. Ο α διαιρείται με τον 2 ή τον 5 αν και μόνο αν το τελευταίο ψηφίο του α διαιρείται με τον 2 ή τον 5, αντίστοιχα.

2. Ο α διαιρείται με τον 4, 20, 25, 50, 100 αν και μόνο αν ο διψήφιος αριθμός που σχηματίζουν τα δύο τελευταία ψηφία του διαιρείται με τον 4, 20, 25, 50, 100 αντίστοιχα.

3. Ο α διαιρείται με τον 3 ή τον 9 αν και μόνο αν το άθροισμα των ψηφίων του α διαιρείται με τον 3 ή τον 9, αντίστοιχα.

4. Ο α διαιρείται με τον 11 αν και μόνο αν η διαφορά του αθροίσματος των ψηφίων του α περιττής τάξης μείον το άθροισμα των ψηφίων του α άρτιας τάξης διαιρείται με τον 11.

Παρατήρηση
Τα κριτήρια διαιρετότητας εξαρτώνται από το σύστημα αρίθμησης που χρησιμοποιούμε. Τα παραπάνω κριτήρια προϋποθέτουν ότι οι αριθμοί είναι γραμμένοι στο δεκαδικό σύστημα.
Στο Κεφάλαιο 2 θα δούμε πώς μπορούμε να κατασκευάσουμε κριτήρια διαιρετότητας για διαίρεση με οποιονδήποτε αριθμό.

Εφαρμογές 1.2

1. Αν α και β είναι δύο περιττοί ακέραιοι αριθμοί τότε $8 \mid \alpha^2 - \beta^2$.

   Απόδειξη.
   Προφανής, αφού γνωρίζουμε ότι οι φυσικοί α^2 και β^2, διαιρούμενοι με τον 8, δίνουν και οι δύο υπόλοιπο υ=1.

2. Για κάθε φυσικό αριθμό ν ο $\nu^3 - \nu$ είναι πολλαπλάσιο του 3.

   Απόδειξη.
   Ο αριθμός $\alpha = \nu^3 - \nu$ γράφεται στη μορφή $\alpha = \nu(\nu^2 - 1) = (\nu - 1)\,\nu\,(\nu + 1)$ άρα, ως γινόμενο τριών διαδοχικών φυσικών, είναι πολλαπλάσιο του 3.

3. Για κάθε φυσικό αριθμό ν, οι αριθμοί $\nu(\nu - 1)$ και $(\nu + 1)^2$ έχουν διαφορετικό άθροισμα ψηφίων.

   Απόδειξη.
   Παρατηρούμε ότι $(\nu + 1)^2 - \nu(\nu - 1) = \nu^2 + 2\nu + 1 - \nu^2 + \nu = 3\nu + 1$ και από την Πρόταση 1.1.2 οι φυσικοί $\nu(\nu - 1)$ και $(\nu + 1)^2$, διαιρούμενοι με τον 3 αφήνουν διαφορετικά υπόλοιπα. Επομένως τα αθροίσματα των ψηφίων τους είναι διαφορετικά.

4. Για κάθε φυσικό αριθμό ν, ένας ακριβώς από τους ν, ν+2 και ν+4 διαιρείται τέλεια με τον αριθμό 3.

   Απόδειξη.
   Ο φυσικός ν μπορεί να γραφεί σε μία από τις μορφές: $\nu = 3x$, $\nu = 3x + 1$ ή $\nu = 3x + 2$.

   (i) Αν ν=3x, τότε $3 \mid \nu$.

   (ii) Αν ν=3x+1, τότε $\nu + 2 = 3x + 3 = 3(x + 1)$ και $3 \mid (\nu + 2)$.

   (iii) Αν ν=3x+2, τότε $\nu + 4 = 3x + 6 = 3(x + 2)$ και $3 \mid (\nu + 4)$.

5. Να αποδειχθεί ότι για κάθε φυσικό ν, ο αριθμός $\nu(\nu^2 + 2)$ είναι πολλαπλάσιο του 3.

   Απόδειξη.
   Εξετάζουμε τρεις περιπτώσεις:

(i) Αν $\nu = 3\kappa$, τότε $\nu(\nu^2+2) = 3\kappa(9\kappa^2+2)$.

(ii) Αν $\nu = 3\kappa+1$, τότε

$$\begin{aligned}\nu(\nu^2+2) &= (3\kappa+1)(9\kappa^2+6\kappa+3)\\ &= 3(3\kappa+1)(3\kappa^2+2\kappa+1).\end{aligned}$$

(iii) Αν $\nu = 3\kappa+2$, τότε

$$\begin{aligned}\nu(\nu^2+2) &= (3\kappa+2)(9\kappa^2+12\kappa+6)\\ &= 3(3\kappa+2)(3\kappa^2+4\kappa+2).\end{aligned}$$

Άρα σε κάθε περίπτωση ο αριθμός $\nu(\nu^2+2)$ είναι πολλαπλάσιο του 3.

6. Για κάθε φυσικό ν να αποδείξετε ότι ο $N = 3^{2\nu+1}+2^{\nu+2}$ είναι πολλαπλάσιο του 7.

Απόδειξη.
(α΄ τρόπος) Από το Θεώρημα 1.1.3 γνωρίζουμε ότι ο φυσικός $3^{2\nu+1} = 3\cdot 9^\nu$ διαιρούμενος με τον 7 δίνει το ίδιο υπόλοιπο με τον $3\cdot 2^\nu$. Επομένως ο $N = 3^{2\nu+1}+2^{\nu+2}$ διαιρούμενος με τον 7 είναι ισοϋπόλοιπος με τον $3\cdot 2^\nu + 2^{\nu+2} = 7\cdot 2^\nu$. Άρα ο αριθμός N είναι πολλαπλάσιο του 7.
(β΄ τρόπος) Είναι διαδοχικά:

$$\begin{aligned}3^{2\nu+1}+2^{\nu+2} &= 3\cdot 3^{2\nu}+4\cdot 2^\nu\\ &= 3\cdot 9^\nu + (7\cdot 2^\nu - 3\cdot 2^\nu)\\ &= 3(9^\nu - 2^\nu)+7\cdot 2^\nu\\ &= 3(9-2)(9^{\nu-1}+9^{\nu-2}\cdot 2+\ldots+2^{\nu-1})+7\cdot 2^\nu\\ &= 7\varkappa.\end{aligned}$$

όπου $\varkappa = 3(9^{\nu-1}+9^{\nu-2}+\ldots+2^{\nu-1})+2^\nu$.

7. Να αποδειχθεί ότι για κάθε φυσικό ν, ο $N = \nu^5 - 5\nu^3 + 4\nu$ είναι πολλαπλάσιο του 8.

   Απόδειξη.
   Ο αριθμός N γράφεται ως :

$$\begin{aligned} N &= \nu^5 - 5\nu^3 + 4\nu \\ &= \nu(\nu^4 - 5\nu^2 + 4) \\ &= \nu(\nu^2 - 1)(\nu^2 - 4) \\ &= \nu(\nu - 1)(\nu + 1)(\nu - 2)(\nu + 2). \end{aligned}$$

   Δηλαδή, ο N είναι το γινόμενο πέντε διαδοχικών ακεραίων. Ανάμεσά τους υπάρχουν τουλάχιστον δύο άρτιοι από τους οποίους ο ένας είναι σίγουρα πολλαπλάσιο του 4. Άρα ο N είναι πολλαπλάσιο του $2 \cdot 4 = 8$.

8. Να αποδειχθεί ότι $25 \mid (16^\nu + 10\nu - 1)$ για κάθε φυσικό ν.

   Απόδειξη.
   Παρατηρούμε ότι

$$\begin{aligned} 16^\nu &= (15+1)^\nu \\ &= 15^\nu + \nu \cdot 15^{\nu-1} + \ldots + \nu \cdot 15 + 1 \\ &= 3^\nu \cdot 5^\nu + \nu \cdot 3^{\nu-1} \cdot 5^{\nu-1} + \ldots + \nu \cdot 15 + 1 \\ &= 25\kappa + 15\nu + 1, \end{aligned}$$

   για κατάλληλο φυσικό κ.
   Άρα $16^\nu + 10\nu - 1 = 25\kappa + 25\nu = 25(\kappa + \nu)$ και $25 \mid (16^\nu + 10\nu - 1)$.

9. Έστω α και β δυό περιττοί φυσικοί. Να αποδειχθεί ότι $2^\kappa \mid (\alpha^3 - \beta^3)$ αν και μόνο αν $2^\kappa \mid (\alpha - \beta)$.

   Απόδειξη.
   Αν $2^\kappa \mid (\alpha - \beta)$, τότε ο 2^κ διαιρεί και τον αριθμό $\alpha^3 - \beta^3 = (\alpha - \beta)(\alpha^2 + \alpha\beta + \beta^2)$, αφού ο αριθμός $\alpha^2 + \alpha\beta + \beta^2$ είναι ακέραιος.
   Αντίστροφα, ας υποθέσουμε ότι $2^\kappa \mid (\alpha^3 - \beta^3)$. Ο αριθμός $\alpha^3 - \beta^3$ γράφεται $\alpha^3 - \beta^3 = (\alpha - \beta)(\alpha^2 + \alpha\beta + \beta^2)$.
   Επειδή ο $\alpha^2 + \alpha\beta + \beta^2$ είναι περιττός, δεν θα διαιρείται από τον 2^κ, οπότε $2^\kappa \mid (\alpha - \beta)$.

10. Να αποδειχθεί ότι για κάθε φυσικό ν, ισχύει ότι $9 \mid (2^{4\nu+1} - 2^{2\nu} - 1)$.

Απόδειξη.
Παρατηρούμε ότι

$$\begin{aligned} 2^{4\nu+1} - 2^{2\nu} - 1 &= (2^{2\nu} - 1)(2^{2\nu+1} + 1) \\ &= (4^{\nu} - 1)(2^{2\nu+1} + 1) \\ &= (4 - 1)(4^{\nu-1} + \ldots + 1)(2 + 1) \\ &\quad (2^{2\nu} - 2^{2\nu-1} + \ldots + 1) \\ &= 9(4^{\nu-1} + \ldots + 1)(2^{2\nu} - 2^{2\nu-1} + \ldots, + 1) \end{aligned}$$

Επομένως, ο αριθμός $2^{4\nu+1} - 2^{\nu} - 1$ είναι πολλαπλάσιο του 9.

11. Να αποδείξετε ότι το άθροισμα των τετραγώνων τριών διαδοχικών περιττών φυσικών αυξημένο κατά 1 είναι πολλαπλάσιο του 12.

Απόδειξη.
Θεωρούμε τρεις διαδοχικούς περιττούς

$$2x + 1, 2x + 3, 2x + 5$$

και υπολογίζουμε το άθροισμα των τετραγώνων τους συν 1:

$$\begin{aligned} N &= (2x + 1)^2 + (2x + 3)^2 + (2x + 5)^2 + 1 \\ &= 12x^2 + 36x + 36 \\ &= 12(x^2 + 3x + 3). \end{aligned}$$

Άρα $12 \mid N$.

12. Αν α, β και γ είναι τρεις φυσικοί αριθμοί με $\alpha^2 + \beta^2 = \gamma^2$, να αποδειχθεί ότι $3 \mid \alpha\beta\gamma$.

Απόδειξη.
Γνωρίζουμε ότι το τετράγωνο ενός αριθμού που δεν είναι πολλαπλάσιο του 3 είναι της μορφής $3x + 1$.
Αν υποθέσουμε ότι κανείς από τους φυσικούς α, β, γ δεν είναι πολλαπλάσιο του 3, τότε $\alpha^2 = 3x + 1$, $\beta^2 = 3\lambda + 1$, $\gamma^2 = 3\mu + 1$, για κατάλληλους x, λ, μ. Έτσι προκύπτει ότι $3x + 1 + 3\lambda + 1 = 3\mu + 1$, αδύνατο.
Επομένως, ένας τουλάχιστον από τους α, β, γ είναι πολλαπλάσιο του 3, οπότε $3 \mid \alpha\beta\gamma$.

Ασκήσεις 1.2

Α' Ομάδα

1. Να ολοκληρωθεί η απόδειξη του Θεωρήματος 1.2.1.

2. Βρείτε το πλήθος των θετικών ακεραίων που δεν υπερβαίνουν τον αριθμό 10000 και που διαιρούνται ακριβώς με τον αριθμό:
   (i) 5 (ii) 25 (iii) 125 (iv) 225

3. Πόσοι αριθμοί μεταξύ του 100 και του 1000 διαιρούνται ακριβώς με καθέναν από τους παρακάτω αριθμούς;
   (i) 7 (ii) 17 (iii) 27 (iv) 49

4. Υπάρχουν θετικοί ακέραιοι α, β, γ τέτοιοι ώστε $\alpha \mid \beta \cdot \gamma$, ενώ ο α δεν διαιρεί ούτε τον β ούτε τον γ;

5. Αν α και β είναι δύο ακέραιοι αριθμοί τέτοιοι ώστε $\alpha \mid \beta$, τότε $\alpha^x \mid \beta^x$ για κάθε θετικό ακέραιο x.

6. Να αποδειχθεί ότι :
   (i) Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$, τότε $\alpha^2 \mid \beta\gamma$.
   (ii)Αν $\gamma \neq 0$, τότε $\alpha \mid \beta$ αν και μόνο αν $\alpha\gamma \mid \beta\gamma$.

7. Έστω ένας ακέραιος α που δεν είναι πολλαπλάσιο του 2 ή του 3. Να αποδειχθεί ότι ο α^2 είναι της μορφής $12\nu + 1$.

8. Να αποδειχθούν τα παρακάτω για κάθε φυσικό $\nu \geq 1$.
   (i) $3 \mid (2^{2\nu} - 1)$
   (ii) $(\alpha - \beta) \mid (\alpha^\nu - \beta^\nu)$, για κάθε επιλογή διακεκριμένων ακεραίων α, β.
   (iii)$(\alpha + \beta) \mid (\alpha^{2\nu-1} + \beta^{2\nu-1})$, για κάθε επιλογή ακεραίων α, β.

9. Έστω ν ένας φυσικός αριθμός και α, β δύο διακεκριμένοι ακέραιοι. Να αποδειχθεί ότι $(\alpha + \beta) \mid (\alpha^{2\nu} - \beta^{2\nu})$.

10. Αν ο αριθμός ν δεν είναι πολλαπλάσιο του 5, να αποδειχθεί ότι ο ν^4 είναι της μορφής $5x + 1$.

11. Αν α και β είναι δύο ακέραιοι, όχι πολλαπλάσια του 5, να αποδειχθεί ότι $5 \mid (\alpha^4 - \beta^4)$.

Β' Ομάδα

12. Να αποδειχθεί ότι για κάθε άρτιο φυσικό ν, ο αριθμός $N = 2 + 2^2 + 2^3 + \ldots + 2^{\nu-1} + 2^\nu$ είναι πολλαπλάσιο του 6.

13. Αν ένας ακέραιος α είναι πολλαπλάσιο του 3 αλλά όχι και του 2, να αποδείξετε ότι $4 \mid (\alpha^2 - 1)$.

14. Να αποδείξετε ότι ο αριθμός

$$\frac{2^{4\nu+2} + 1}{5}$$

είναι ακέραιος, για κάθε φυσικό ν.

15. Αν α, β είναι δύο φυσικοί που δε διαιρούνται με τον 3, να αποδειχθεί ότι ο $N = \alpha^2 + \beta^2$ δεν είναι τέλειο τετράγωνο ακεραίου.

16. Να αποδείξετε ότι για κάθε φυσικό ν ισχύει ότι $8^\nu \mid (4\nu)!$ και $16^\nu \mid (6\nu)!$, όπου $\nu! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (\nu - 1) \cdot \nu$.

17. Να αποδειχθεί ότι για κάθε φυσικό ν, ο αριθμός $N = \nu^5 - \nu$ διαιρείται με τον αριθμό 5.

18. Να αποδειχθεί ότι το άθροισμα των κύβων τριών διαδοχικών ακεραίων διαιρείται με τον αριθμό 9.

19. Αν α, κ, ν, δ είναι φυσικοί αριθμοί τέτοιοι ώστε

$$\delta \mid \alpha^{2^\kappa} + 1 \text{ και } \delta \mid \alpha^{2^\nu} - 1,$$

με $\kappa > \nu$, τότε ο δ είναι 1 αν ο α είναι άρτιος και 2 αν ο α είναι περιττός.

20. Έστω α, κ δύο μη-μηδενικοί φυσικοί τέτοιοι ώστε ο αριθμός $\alpha^2 + \kappa$ να διαιρεί τον $(\alpha - 1)\alpha(\alpha + 1)$. Να αποδείξετε ότι $\kappa \geq \alpha$.

21. Έστω x, y δύο διαφορετικοί επταψήφιοι αριθμοί που αποτελούνται απο τα ψηφία 1, 2, 3, 4, 5, 6, 7 χωρίς επαναλήψεις. Να αποδείξετε ότι ο x δεν γίνεται να είναι πολλαπλάσιο του y.

22. Να αποδειχθεί ότι για κάθε φυσικό ν, ο αριθμός $N = 7^{2\nu} - 2352\nu - 1$ είναι πολλαπλάσιο του 2304.

23. Να αποδειχθεί ότι αν $\mu > 1$ και $2^\nu + 1 = \alpha^\mu$, τότε $\mu = 2$.

1.3 Μέγιστος Κοινός Διαιρέτης

Ο **μέγιστος κοινός διαιρέτης** δύο ακεραίων αριθμών α, β προσδιορίζεται ως ο μέγιστος φυσικός κοινός παράγοντάς τους. Ιδιαίτερο ενδιαφέρον παρουσιάζει ο αλγόριθμος εύρεσής του, ο οποίος συνδέει τη διαιρετότητα δύο αριθμών με τη διαιρετότητα των διαδοχικών υπολοίπων τους, ενώ ως αντίστροφη διαδικασία εκφράζει όπως θα δούμε παρακάτω τη γραμμική διοφαντική εξίσωση. Ο μέγιστος κοινός διαιρέτης των α και β συμβολίζεται με $\delta = (\alpha, \beta)$ και αν είναι ίσος με τη μονάδα τότε οι αριθμοί α και β ονομάζονται **πρώτοι μεταξύ τους** ή **σχετικά πρώτοι**. Προφανώς αν $\alpha \mid \beta$, τότε $(\alpha, \beta) = \alpha$.

Πρόταση 1.3.1
Έστω α και β δύο ακέραιοι αριθμοί με $\beta \neq 0$ και υ το υπόλοιπο της διαίρεσης α δια β. Τότε ένας ακέραιος δ διαιρεί τους α και β αν και μόνο αν είναι κοινός διαιρέτης των β και υ.

Απόδειξη.
Από το Θεώρημα 1.2.1(viii) προκύπτει ότι αν ο δ είναι κοινός παράγοντας των α και β, τότε θα είναι και κοινός παράγοντας των α και $\upsilon = \alpha - \pi\beta$. Προφανώς ισχύει και το αντίστροφο.

Πρόταση 1.3.2
Έστω α, β και γ τρεις μη μηδενικοί ακέραιοι αριθμοί. Τότε ισχύουν οι ακόλουθες σχέσεις :
(i) $(\alpha, \beta) = (\beta, \alpha) = (\alpha, -\beta) = (\alpha, \beta + \alpha\gamma)$,
(ii) $(\alpha, (\beta, \gamma)) = ((\alpha, \beta), \gamma)$,
(iii) $(\alpha, 1) = 1$ και $(\alpha, 0) = \alpha$.

Απόδειξη.
Απλή εφαρμογή του ορισμού.

Η ουσιαστική μέθοδος εύρεσης του μέγιστου κοινού διαιρέτη (α, β) είναι ο **αλγόριθμος του Ευκλείδη**. Είναι μια διαδικασία που χρησιμοποιεί διαδοχικές διαιρέσεις και περιγράφεται στο θεώρημα που ακολουθεί.

Πρόταση 1.3.3 (Αλγόριθμος του Ευκλείδη)
Έστω α και β δύο φυσικοί αριθμοί. Θεωρούμε τις εξισώσεις :

$$\begin{aligned}
\alpha &= \pi_1\beta + \upsilon_1, & 0 < \upsilon_1 < \beta \\
\beta &= \pi_2\upsilon_1 + \upsilon_2, & 0 < \upsilon_2 < \upsilon_1 \\
\upsilon_1 &= \pi_3\upsilon_2 + \upsilon_3, & 0 < \upsilon_3 < \upsilon_2 \\
&\vdots \\
\upsilon_{x-2} &= \pi_x\upsilon_{x-1} + \upsilon_x, & 0 < \upsilon_x < \upsilon_{x-1} \\
\upsilon_{x-1} &= \pi_{x+1}\upsilon_x.
\end{aligned}$$

Τότε ο μέγιστος κοινός διαιρέτης των α, β είναι το τελευταίο μη μηδενικό υπόλοιπο υ_x.

Απόδειξη.
Παρατηρούμε ότι όλα τα υπόλοιπα είναι φυσικοί αριθμοί και $\upsilon_1 > \upsilon_2 > \upsilon_3 > \ldots$ Για το λόγο αυτό, η διαδικασία αργά ή γρήγορα καταλήγει σε ένα μηδενικό υπόλοιπο. Αρκεί τώρα να αποδείξουμε πως το υπόλοιπο υ_x ισούται με τον (α, β). Από την Πρόταση 1.3.2(i) έχουμε :

$$\begin{aligned}
(\alpha,\beta) &= (\alpha - \pi_1\beta, \beta) && = (\upsilon_1, \beta) \\
&= (\upsilon_1, \beta - \pi_2\upsilon_1) && = (\upsilon_1, \upsilon_2) \\
&= (\upsilon_1 - \pi_3\upsilon_2, \upsilon_2) && = (\upsilon_3, \upsilon_2) \\
&\vdots \\
&= (\upsilon_{x-3} - \pi_{x-1}\upsilon_{x-2}, \upsilon_{x-2}) && = (\upsilon_{x-1}, \upsilon_{x-2}) \\
&= (\upsilon_{x-1}, \upsilon_{x-2} - \pi_x\upsilon_{x-1}) && = (\upsilon_{x-1}, \upsilon_x) \\
&= \upsilon_x.
\end{aligned}$$

Στις εξισώσεις της προηγούμενης πρότασης μπορούμε να λύσουμε ως προς υ_x με απαλοιφή των υπολοίπων:

$$\upsilon_{x-1}, \upsilon_{x-2}, \ldots, \upsilon_2, \upsilon_1$$

ακολουθώντας την αντίστροφη πορεία. Έτσι, ο $\upsilon_x = (\alpha, \beta)$ μπορεί να γραφεί ως γραμμικός συνδυασμός των α και β. Καταλήγουμε λοιπόν στο παρακάτω σημαντικό αποτέλεσμα:

Θεώρημα 1.3.4
Αν δ είναι ο μέγιστος κοινός διαιρέτης των α και β, τότε υπάρχουν ακέραιοι κ και λ τέτοιοι ώστε $\delta = (\alpha, \beta) = \kappa\alpha + \lambda\beta$.

Στην περίπτωση που ο δ είναι ίσος με τη μονάδα, ισχύει και το αντίστροφο, όπως αποδεικνύεται στο παρακάτω θεώρημα.

Πόρισμα 1.3.5

Δύο ακέραιοι αριθμοί α και β είναι πρώτοι μεταξύ τους αν και μόνο αν υπάρχουν ακέραιοι κ και λ τέτοιοι ώστε $\kappa\alpha + \lambda\beta = 1$.

Απόδειξη.

Αν οι ακέραιοι α και β είναι πρώτοι μεταξύ τους τότε $(\alpha, \beta) = 1$ και από το Θεώρημα 1.3.4 υπάρχουν ακέραιοι κ και λ τέτοιοι ώστε $\kappa\alpha + \lambda\beta = 1$. Αντίστροφα, αν υπάρχουν κ, λ με $\kappa\alpha + \lambda\beta = 1$ και $\delta = (\alpha, \beta)$, τότε $\delta|\alpha$ και $\delta|\beta$. Επομένως $\delta|(\kappa\alpha + \lambda\beta)$, δηλαδή $\delta \mid 1$ ή $\delta = 1$.

Παράδειγμα

Εύρεση του Μ.Κ.Δ. των 567 και 392.

$$\begin{aligned} 567 &= 1 \cdot 392 + 175 \quad (\beta\acute{\eta}\mu\alpha\ 1) \\ 392 &= 2 \cdot 175 + 42 \quad (\beta\acute{\eta}\mu\alpha\ 2) \\ 175 &= 4 \cdot 42 + 7 \quad (\beta\acute{\eta}\mu\alpha\ 3) \\ 42 &= 6 \cdot 7 \end{aligned}$$

Άρα (567, 392)=7.

Επαλήθευση: Είναι $567 = 3 \cdot 3 \cdot 3 \cdot 3 \cdot 7$ και $392 = 2 \cdot 2 \cdot 2 \cdot 7 \cdot 7$.

Πράγματι, ο αριθμός 7 είναι ο μοναδικός κοινός διαιρέτης των δύο αριθμών, μεγαλύτερος του 1, οπότε ο Μ.Κ.Δ. είναι 7.
Για να βρούμε τους αριθμούς κ, λ του Θεωρήματος 1.3.4 εργαζόμαστε ως εξής:

$$\begin{aligned} 7 &= 175 - 4 \cdot 42 && (\alpha\pi\acute{o}\ \tau o\ \beta\acute{\eta}\mu\alpha\ 3) \\ &= 175 - 4(392 - 2 \cdot 175) && (\alpha\pi\acute{o}\ \tau o\ \beta\acute{\eta}\mu\alpha\ 2) \\ &= -4 \cdot 392 + 9 \cdot 175 \\ &= -4 \cdot 392 + 9(567 - 392) && (\alpha\pi\acute{o}\ \tau o\ \beta\acute{\eta}\mu\alpha\ 1) \\ &= 9 \cdot 567 - 13 \cdot 392 \end{aligned}$$

Ο αλγόριθμος του Ευκλείδη είναι ένας πολύ αποτελεσματικός τρόπος εύρεσης του Μ.Κ.Δ., ακόμα και για μεγάλους αριθμούς. Ο αριθμός των βημάτων που χρειάζεται για να βρούμε τον Μ.Κ.Δ. με τον αλγόριθμο

του Ευκλείδη είναι το πολύ 5 φορές το πλήθος των ψηφίων του μικρότερου από τους αριθμούς[1].

Σχόλιο
Ο αλγόριθμος του Ευκλείδη και οι πράξεις για την εύρεση των αριθμών κ, λ τέτοιων ώστε $\delta = \kappa\alpha + \lambda\beta$ μπορούν να παρασταθούν με τη μορφή πίνακα, όπως φαίνεται παρακάτω. Για παράδειγμα για το $(37, 10) = 1$ έχουμε

$$\begin{aligned} 37 &= 3 \cdot 10 + 7 \\ 10 &= 1 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 \end{aligned}$$

και $1 = 7-2\cdot 3 = 7-2(10-1\cdot 7) = -2\cdot 10+3\cdot(37-3\cdot 10) = 3\cdot 37-11\cdot 10$. Στην πρώτη γραμμή τοποθετούμε τα υπόλοιπα ενώ στην τελευταία τα πηλίκα των διαιρέσεων δύο διαδοχικών αριθμών της μεσαίας γραμμής.

		$\upsilon\pi o\lambda(x\ :\ y)$		
...	x	y	$\upsilon\pi o\lambda(x\ :\ y)$	...
		$\pi\eta\lambda\acute{\iota}\kappa o(x\ :\ y)$		

	7	3	1	0	*υπόλοιπα*
37	10	7	3	1	
	3	1	2	3	*πηλίκα*

Η διαδικασία τελειώνει όταν το υπόλοιπο γίνει μηδέν και ο μέγιστος κοινός διαιρέτης είναι το τελευταίο μη μηδενικό υπόλοιπο. Για να βρούμε τους κ, λ γράφουμε τα πηλίκα που βρήκαμε με αντίθετο πρόσημο και ακολουθούμε την αντίστροφη διαδικασία, συμπληρώνοντας την πρώτη στήλη με τους αριθμούς 1, 0 αρχικά.

1		υ	α	
0	...	α	$\alpha\pi + \upsilon$	...
		π		

[1] Η χειρότερη περίπτωση συμβαίνει όταν οι αριθμοί είναι διαδοχικοί αριθμοί Fibonacci.

1	0	1	−2	3
0	1	−2	3	−11
−3	−2	−1	−3	

Οι ζητούμενοι αριθμοί είναι οι δύο τελευταίοι της μεσαίας στήλης, δηλαδή $1 = 3 \cdot 37 + (-11) \cdot 10$.
Η παραπάνω διάταξη αναφέρεται ως "μέθοδος Αυδή", αφού ο Ι. Αυδής την περιέγραψε πρώτος στην Ελληνική βιβλιογραφία.

Εκμεταλλευόμενοι το "μέγιστο" είμαστε σε θέση να δώσουμε έναν ισοδύναμο ορισμό για τον μέγιστο κοινό διαιρέτη δύο ακεραίων αριθμών.

Θεώρημα 1.3.6
Έστω δύο ακέραιοι αριθμοί α, β και δ ένας θετικός κοινός διαιρέτης τους. Τότε ο δ είναι ο μέγιστος κοινός διαιρέτης των α και β αν και μόνο αν για κάθε θετικό κοινό διαιρέτη δ' των α και β ισχύει $\delta' \mid \delta$.

Απόδειξη.
Αν $\delta = (\alpha, \beta)$, τότε από το Θεώρημα 1.3.4 θα γράφεται $\delta = \kappa\alpha + \lambda\beta$ όπου κ και λ είναι κατάλληλοι ακέραιοι. Επομένως, για κάθε δ' με $\delta' \mid \alpha$ και $\delta' \mid \beta$ έχουμε $\delta' \mid (\kappa\alpha + \lambda\beta)$ και $\delta' \mid \delta$. Αντίστροφα, αν υποθέσουμε ότι ο δ είναι ένας θετικός κοινός διαιρέτης των α και β, τέτοιος ώστε $\delta' \mid \delta$ για κάθε κοινό διαιρέτη δ' των α και β, τότε είναι προφανές ότι $\delta' \leq \delta$ και δ=(α,β).

Το παραπάνω θεώρημα αποδεικνύει επιπλέον ότι ο μέγιστος κοινός διαιρέτης δύο αριθμών είναι μοναδικός. Πράγματι, αν δ_1 και δ_2 είναι δύο μέγιστοι κοινοί διαιρέτες των α και β, τότε $\delta_1 \mid \delta_2$ και $\delta_2 \mid \delta_1$. Άρα από την Πρόταση 1.2.1(i) ισχύει $\delta_1 = \delta_2$, δηλαδή ο Μ.Κ.Δ. δύο αριθμών είναι μοναδικός.

Η σχέση της πράξης του πολλαπλασιασμού με τον Μ.Κ.Δ. εκφράζεται από την ακόλουθη πρόταση :

Πρόταση 1.3.7
Έστω α, β και γ τρεις ακέραιοι αριθμοί, με $\gamma > 0$. Τότε ισχύουν τα εξής:
(i) $(\alpha\gamma, \beta\gamma) = \gamma \cdot (\alpha, \beta)$.
(ii) Αν $\gamma \mid \alpha$ και $\gamma \mid \beta$, τότε $(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}) = \frac{1}{\gamma}(\alpha,\beta)$.

Απόδειξη.
(i) Ας θεωρήσουμε $\delta_1 = (\alpha, \beta)$ και $\delta_2 = (\alpha\gamma, \beta\gamma)$. Προφανώς $\gamma\delta_1 \mid \alpha\gamma$ και $\gamma\delta_1 \mid \beta\gamma$, δηλαδή $\gamma\delta_1 \mid \delta_2$, από το Θεώρημα 1.3.6. Ακόμη $\gamma(\alpha, \beta) = \kappa\alpha\gamma + \lambda\beta\gamma$ για κατάλληλους ακεραίους κ και λ. Επομένως $\delta_2 \mid (\kappa\alpha\gamma + \lambda\beta\gamma)$ ή $\delta_2 \mid \gamma\delta_1$ και τελικά προκύπτει ότι $\delta_2 = \gamma\delta_1$.
(ii) Η απόδειξη είναι άμεση συνέπεια του (i).

Από το μέρος (ii) της παραπάνω πρότασης είναι προφανές το ακόλουθο πόρισμα.

Πόρισμα 1.3.8
Αν $\delta = (\alpha, \beta)$ είναι ο μέγιστος κοινός διαιρέτης των α και β, τότε οι αριθμοί α/δ και β/δ είναι πρώτοι μεταξύ τους, δηλαδή $\left(\frac{\alpha}{\delta}, \frac{\beta}{\delta}\right) = 1$.

Με τη χρήση της έννοιας του Μ.Κ.Δ. μπορούμε να αποδείξουμε ένα ισχυρό θεώρημα στη διαιρετότητα:

Θεώρημα 1.3.9 (Λήμμα του Ευκλείδη)
Αν για τους ακεραίους α, β και γ ισχύει $\gamma \mid \alpha\beta$ και $(\gamma, \alpha) = 1$, τότε $\gamma \mid \beta$.

Απόδειξη.
Αφού $(\gamma, \alpha) = 1$ από την Πρόταση 1.3.7(i) έχουμε ότι $(\gamma\beta, \alpha\beta) = \beta$. Όμως $\gamma \mid \gamma\beta$ και $\gamma \mid \alpha\beta$, δηλαδή ο γ είναι κοινός διαιρέτης των $\gamma\beta$ και $\alpha\beta$ και από το Θεώρημα 1.3.6 προκύπτει ότι $\gamma \mid \beta$.

Με τη βοήθεια του Λήμματος του Ευκλείδη οδηγούμαστε σε αρκετά σημαντικά αποτελέσματα, όπως τα ακόλουθα:

Πρόταση 1.3.10
Αν για τους ακεραίους α, β και γ ισχύει $\alpha \mid \gamma$, $\beta \mid \gamma$ και $(\alpha, \beta) = 1$, τότε $\alpha\beta \mid \gamma$.

Απόδειξη.
Αφού $\alpha \mid \gamma$ θα υπάρχει ακέραιος αριθμός κ τέτοιος ώστε $\gamma = \kappa\alpha$. Επομένως $\beta \mid \kappa\alpha$ με $(\alpha, \beta) = 1$, άρα από την Πρόταση 1.3.9 έχουμε ότι $\beta \mid \kappa$. Τελικά από το Θεώρημα 1.2.1(v) προκύπτει ότι $\alpha\beta \mid \alpha\kappa$ ή $\alpha\beta \mid \gamma$.

Σχόλιο
Στην επόμενη παράγραφο θα δούμε γενικότερα ότι αν $\alpha \mid \gamma$, $\beta \mid \gamma$ τότε το ελάχιστο κοινό πολλαπλάσιο των α, β διαιρεί τον γ.

Πρόταση 1.3.11
Αν για τους ακεραίους α, β και γ ισχύει $(\alpha, \beta) = \delta$ και $(\beta, \gamma) = 1$, τότε $(\alpha \cdot \gamma, \beta) = \delta$.

Απόδειξη.
Ο δ ως μέγιστος κοινός διαιρέτης των ακεραίων α και β θα είναι κοινός διαιρέτης και των $\alpha\gamma$ και β. Ακόμη αν δ' είναι ένας κοινός διαιρέτης των $\alpha\gamma$ και β, τότε από το Θεώρημα 1.3.9, ο δ' είναι κοινός διαιρέτης των α και β διότι $(\beta, \gamma) = 1$. Άρα $\delta' \mid \delta$ και $\delta = (\alpha\gamma, \beta)$.

Εφαρμογές 1.3

1. Με την βοήθεια του αλγόριθμου του Ευκλείδη να υπολογισθεί ο μέγιστος κοινός διαιρέτης των αριθμών 3999 και 7026.

   Λύση.
   Εφαρμόζοντας τον αλγόριθμο του Ευκλείδη που περιγράφεται στην Πρόταση 1.3.3 έχουμε:

$$\begin{aligned} 7026 &= 1 \cdot 3999 + 3027 \\ 3999 &= 1 \cdot 3027 + 972 \\ 3027 &= 3 \cdot 972 + 111 \\ 972 &= 8 \cdot 111 + 84 \\ 111 &= 1 \cdot 84 + 27 \\ 84 &= 3 \cdot 27 + 3 \\ 27 &= 9 \cdot 3 + 0. \end{aligned}$$

   Επομένως,$(3999, 7026) = 3$.

2. Να γραφεί ο μέγιστος κοινός διαιρέτης (3999, 7027) ως γραμμικός συνδυασμός των αριθμών 3999 και 7027.

   Λύση.
   Θεωρούμε τις εξισώσεις του αλγορίθμου του Ευκλείδη που είχαμε στην προηγούμενη εφαρμογή.
   Ακολουθώντας την αντίστροφη πορεία αυτών των εξισώσεων και λύνοντας καθεμιά τους ως προς το αντίστοιχο υπόλοιπο, έχουμε:

$$\begin{aligned} 3 &= 84 - 3 \cdot 27 = 84 - 3(111 - 84) \\ &= -3 \cdot 111 + 4(972 - 8 \cdot 111) \\ &= 4 \cdot 972 - 35(3027 - 3 \cdot 972) \\ &= -35 \cdot 3027 + 109(3999 - 3027) \\ &= 109 \cdot 3999 - 144(7026 - 3999) \\ &= 253 \cdot 3999 - 144 \cdot 7026 \end{aligned}$$

   Άρα $3 = (3999, 7026) = 253 \cdot 3999 - 144 \cdot 7026$.

Παρατήρηση
Με την μέθοδο Ανδή έχουμε ότι :

	3027	972	111	84	27	3	0
7026	3999	3027	972	111	84	27	3
	1	1	3	8	1	3	9

1	0	1	−3	4	−35	109	
0	1	−3	4	−35	109	−144	253
−9	−3	−1	−8	−3	−1	−1	

3. Να αποδειχθεί ότι κάθε φυσικός αριθμός $\nu \geq 2$ είναι σχετικά πρώτος με τον επόμενο φυσικό $\nu + 1$.

   Απόδειξη.
   Ας υποθέσουμε πως υπάρχει κοινός διαιρέτης $\delta > 1$ των αριθμών ν και $\nu + 1$. Τότε ο δ είναι διαιρέτης και της διαφοράς $(\nu + 1) - \nu$, δηλαδή $\delta \mid 1$, το οποίο είναι άτοπο.

4. Να αποδείξετε ότι για κάθε ακέραιο ν ισχύει $(2\nu + 1, 9\nu + 4) = 1$.

   Απόδειξη.
   Αρκεί να βρούμε δύο ακέραιους αριθμούς x και y, τέτοιους ώστε:

   $$x(2\nu + 1) + y(9\nu + 4) = 1 \ \text{ή} \ (2x + 9y)\nu + x + 4y = 1 \ ,$$

   για κάθε ακέραιο ν. Για $\nu = 1$ πρέπει $3x + 13y = 1$, ενώ για $\nu = 2$ πρέπει $5x + 22y = 1$.

   Οι ακέραιοι $x = 9$ και $y = -2$ ικανοποιούν τις παραπάνω εξισώσεις, αλλά και την εξίσωση $(2x + 9y)\nu + (x + 4y) = 1$, για κάθε ακέραιο ν, όπως εύκολα επαληθεύουμε.

5. Έστω α και β δύο φυσικοί, τέτοιοι ώστε $(\alpha, 4) = 2$ και $(\beta, 4) = 2$. Να αποδείξετε ότι $(\alpha + \beta, 4) = 4$.

   Απόδειξη.
   Οι αριθμοί α και β είναι άρτιοι, αλλά όχι πολλαπλάσια του 4. Επομένως είναι της μορφής $\alpha = 4\nu + 2$ και $\beta = 4\kappa + 2$ για κατάλληλους φυσικούς ν και κ. Άρα το άθροισμα $\alpha + \beta = 4\nu + 2 + 4\kappa + 2 = 4(\nu + \kappa + 1)$ είναι πολλαπλάσιο του 4 οπότε $(\alpha + \beta, 4) = 4$.

6. Να βρεθούν φυσικοί μ και ν τέτοιοι ώστε $(\mu, \nu) = 36$ και $\mu + \nu = 432$.

   Λύση.
   Αφού οι φυσικοί μ και ν είναι πολλαπλάσια του 36, γράφονται $\mu = 36\alpha$ και $\nu = 36\beta$. Επομένως από τη σχέση μ+ν=432, προκύπτει ότι $36\alpha + 36\beta = 432$ ή $\alpha + \beta = 12$. Επιπλέον πρέπει (α,β)=1, οπότε $\alpha = 1, \beta = 11$ ή $\alpha = 5, \beta = 7$ ή $\alpha = 7, \beta = 5$ ή $\alpha = 11, \beta = 1$.
   Άρα $\mu = 36$, $\nu = 369$ ή $\mu = 180$, $\nu = 252$ ή $\mu = 252$, $\nu = 180$ ή $\mu = 369$, $\nu = 36$.

7. Να αποδειχθεί ότι για κάθε φυσικό κ, οι αριθμοί $6\kappa - 1$, $6\kappa + 1$, $6\kappa + 2$, $6\kappa + 3$ και $6\kappa + 5$ είναι ανά δύο πρώτοι μεταξύ τους.

   Απόδειξη.
   Για έναν τυχαίο φυσικό κ, θεωρούμε τους $6\kappa - 1$ και $6\kappa + 1$. Προφανώς, αν $\delta = (6\kappa - 1, 6\kappa + 1)$, τότε $\delta \mid [(6\kappa + 1) - (6\kappa - 1)]$, δηλαδή $\delta \mid 2$. Άρα $\delta = 1$ ή $\delta = 2$ και αφού οι αριθμοί $6\kappa - 1$ και $6\kappa + 1$ είναι περιττοί, καταλήγουμε στο ότι $\delta = 1$.
   Όμοια αποδεικνύεται ότι, κάθε ζεύγος από τους $6\kappa - 1$, $6\kappa + 1$, $6\kappa + 2$, $6\kappa + 3$ και $6\kappa + 5$ είναι αριθμοί πρώτοι μεταξύ τους.

8. Αν για τρεις φυσικούς αριθμούς α, β και γ ισχύει $(\alpha, \beta) = 1$, τότε να αποδειχθεί ότι $(\alpha, \gamma) \cdot (\beta, \gamma) = (\alpha\beta, \gamma)$.

   Απόδειξη.
   Προφανώς $(\alpha, \gamma) \mid \alpha\beta$, $(\beta, \gamma) \mid \alpha\beta$, $(\alpha, \gamma) \mid \gamma$ και $(\beta, \gamma) \mid \gamma$ και από τη σχέση $(\alpha, \beta) = 1$ προκύπτει ότι $((\alpha, \gamma), (\beta, \gamma)) = 1$. Άρα από την Πρόταση 1.3.10 έχουμε $(\alpha, \gamma) \cdot (\beta, \gamma) \mid (\alpha\beta, \gamma)$.
   Αν τώρα θεωρήσουμε έναν κοινό διαιρέτη κ των $\alpha\beta$ και γ, τότε ή $\kappa \mid \gamma$ και $\kappa \mid \alpha$ ή $\kappa \mid \gamma$ και $\kappa \mid \beta$, διότι $(\alpha, \beta) = 1$. Επομένως, $\kappa \mid (\alpha, \gamma)$ ή $\kappa \mid (\beta, \gamma)$, οπότε $\kappa \mid (\alpha, \gamma) \cdot (\beta, \gamma)$.
   Δηλαδή το γινόμενο $(\alpha, \beta) \cdot (\beta, \gamma)$ ισούται με τον μέγιστο κοινό διαιρέτη $(\alpha\beta, \gamma)$.

9. Να αποδειχθεί ότι για κάθε φυσικό ν, ο μέγιστος κοινός διαιρέτης των $\nu^2 + 1$ και $(\nu + 1)^2 + 1$ είναι 1 ή 5.

   Απόδειξη.
   Για ν=1 ή 2 έχουμε $(1^2 + 1, (1 + 1)^2 + 1) = (2, 5) = 1$ και

$(2^2+1,(2+1)^2+1)=(5,10)=5$ αντίστοιχα.
Για $\nu>2$ είναι φανερό ότι κάθε κοινός διαιρέτης δ των ν^2+1 και $(\nu+1)^2$ διαιρεί τέλεια και τη διαφορά τους

$$(\nu+1)^2+1-(\nu^2+1)=2\nu+1.$$

Άρα ο δ διαιρεί και τον αριθμό $4(\nu^2+1)-(2\nu+1)(2\nu-1)=5$, οπότε για $\nu>2$, έχουμε $(\nu^2+1,(\nu+1)^2+1)=5$ ή 1.

10. Αν μ και ν είναι δύο τυχαίοι ακέραιοι, να αποδειχθεί ότι ο $N=\mu\cdot\nu\cdot(\mu^4-\nu^4)$ είναι πάντα πολλαπλάσιο του 30.

Αποδειξη.
Ο αριθμός N γράφεται

$$N=\mu\cdot\nu\cdot(\mu^4-\nu^4)=\mu\cdot\nu\cdot(\mu-\nu)(\mu+\nu)(\mu^2+\nu^2)$$

Αρκεί να αποδείξουμε ότι ο N διαιρείται με τους 2, 3 και 5, αφού οι 2, 3, 5 είναι ανά δύο πρώτοι μεταξύ τους.
Αρχικά παρατηρούμε ότι αν ένας από τους μ και ν είναι άρτιος, τότε ο N είναι άρτιος. Επιπλέον, αν οι αριθμοί μ και ν είναι περιττοί τότε ο $\mu+\nu$ είναι άρτιος άρα και ο N θα είναι άρτιος.
Αν ένας από τους μ και ν είναι πολλαπλάσιο του 3, τότε προφανώς $3\mid N$. Αν κανείς από τους μ και ν δεν είναι πολλαπλάσιο του 3, τότε διακρίνουμε περιπτώσεις:

(i) αν $\mu=3\kappa+1$ και $\nu=3\lambda+1$, τότε $3\mid(\mu-\nu)$,

(ii) αν $\mu=3\kappa+1$ και $\nu=3\lambda+2$, τότε $3\mid(\mu+\nu)$,

(iii)αν $\mu=3\kappa+2$ και $\nu=3\lambda+1$, τότε $3\mid(\mu+\nu)$,

(iv)αν $\mu=3\kappa+2$ και $\nu=3\lambda+2$, τότε $3\mid(\mu-\nu)$.

Άρα πάντα ο αριθμός N είναι πολλαπλάσιο του 3.
Τέλος αν ένας από τους μ και ν είναι πολλαπλάσιο του 5, τότε και ο N είναι πολλαπλάσιο του 5. Διαφορετικά εξετάζοντας περιπτώσεις, όπως ακριβώς στο προηγούμενο βήμα, διαπιστώνουμε ότι πάντα $\mu^4=5\kappa+1$ και $\nu^4=5\lambda+1$, οπότε $5\mid(\mu^4-\nu^4)$.
Έτσι καταλήγουμε στο ότι ο N είναι πολλαπλάσιο των 2,3 και 5, οπότε $30\mid N$.

Ασκήσεις 1.3

Α' Ομάδα

1. Να αποδειχθεί ότι για κάθε φυσικό ν, ισχύει $(2\nu - 1, 2\nu + 1) = 1$.

2. Να αποδειχθεί ότι το γινόμενο τριων διαδοχικών αριθμών είναι πάντα πολλαπλάσιο του 6.

3. Να αποδείξετε ότι ο αριθμός $\nu(\nu - 1)(2\nu - 1)$ διαιρείται με τον 6, για κάθε φυσικό ν.

4. Με τη βοήθεια του αλγόριθμου του Ευκλείδη να υπολογισθεί ο μέγιστος κοινός διαιρέτης των αριθμών :
(i)1109 και 4999, (ii) 2378 και 1769.

5. Για κάθε ζεύγος φυσικών αριθμών α, β της προηγούμενης άσκησης να γραφεί ο μέγιστος κοινός διαιρέτης (α, β) ως γραμμικός συνδυασμός των α, β.

6. Να αποδείξετε ότι $(\alpha+\beta, \alpha-\beta) \geq (\alpha, \beta)$, για κάθε ζεύγος φυσικών α και β.

7. Να αποδειχθεί ότι $(\alpha, \alpha + \nu) \mid \nu$ για κάθε ζεύγος θετικών ακεραίων α, ν.

8. Έστω ένας φυσικός αριθμός κ. Αν $(\nu, \nu + \kappa) = 1$ για κάθε φυσικό ν, να αποδείξετε ότι $\kappa = 1$.

9. Να αποδειχθεί ότι δεν υπάρχουν φυσικοί ν και κ, τέτοιοι ώστε ν+κ=100 και (ν,κ)=3.

10. Να αποδειχθούν οι παρακάτω ιδιότητες του μέγιστου κοινού διαιρέτη:
    (i) Αν $(\alpha, \beta) = 1$ και $\gamma \mid \alpha$, τότε $(\beta, \gamma) = 1$.
    (ii) Αν $(\alpha, \beta\gamma) = 1$, τότε $(\alpha, \beta) = (\alpha, \gamma) = 1$.
    (iii)Αν $(\alpha, \beta) = 1$, τότε $(\gamma\alpha, \beta) = (\gamma, \beta)$.

Β' Ομάδα

11. Να αποδειχθεί ότι οι $\alpha = 14\kappa + 3$ και $\beta = 21\kappa + 1$ είναι πρώτοι μεταξύ τους, για κάθε επιλογή του ακεραίου κ.

12. Αν για τους ακέραιους α, β και γ ισχύει

$$(\alpha, \beta) = (\beta, \gamma) = (\alpha, \gamma) = 1,$$

τότε να αποδειχθεί ότι :
(i) $(\alpha, \beta\gamma)=1$ και
(ii) $(\alpha^\kappa, \beta^\nu\gamma^\mu) = 1$ για κάθε τριάδα φυσικών (κ,ν,μ).

13. Αν οι ακέραιοι α και β είναι πρώτοι μεταξύ τους, να αποδείξετε ότι $(\alpha + \beta, \alpha - \beta) = 1$ ή 2.

14. Αν οι ακέραιοι α και β είναι πρώτοι μεταξύ τους, να αποδείξετε ότι $(\alpha + \kappa\beta, \beta) = 1$ για κάθε ακέραιο κ.

15. Για δύο τυχαίους ακεραίους α, β να αποδειχθούν οι σχέσεις:

(i) $(8\alpha + 5, 5\alpha + 3) = 1$

(ii) $(\alpha - \beta, 2\alpha - 3\beta) = (\alpha, \beta)$

16. Για δύο τυχαίους ακεραίους α και β να αποδειχθεί ότι:

(i) $(\alpha + \beta, 5\alpha + 5\beta) = (\alpha, \beta)$

(ii) $(2\alpha + 3\beta, 3\alpha + 4\beta) = (\alpha, \beta)$.

17. Να αποδειχθεί ότι:

(i) $(\alpha, \beta) = 2(\frac{\alpha}{2}, \frac{\beta}{2})$, αν οι α και β είναι άρτιοι ακέραιοι.

(ii)$(\alpha, \beta) = (\alpha, \frac{\beta}{2})$, αν ο α είναι περιττός και ο β είναι άρτιος.

18. Ένα κλάσμα $\frac{\alpha}{\beta}$ καλείται ανάγωγο όταν $(\alpha, \beta) = 1$. Να αποδειχθεί ότι το άθροισμα δύο ανάγωγων κλασμάτων $\frac{\alpha}{\beta}$ και $\frac{\gamma}{\delta}$ με $\beta \neq \delta$ δεν είναι ποτέ ακέραιος.

19. Αν α, β είναι δύο φυσικοί αριθμοί με $(\alpha, 6) = (\beta, 6) = 1$, να αποδειχθεί ότι

    (i) $(\alpha^2 - \beta^2, 12) = 12$

    (ii) $(\alpha^2 + \beta^2, 12) = 2$.

20. Να αποδειχθεί ότι υπάρχουν άπειροι ακέραιοι x και y τέτοιοι ώστε $x + y = 100$ και $(x, y) = 5$.

21. Να αποδειχθεί ότι $30 \mid (\nu^5 - \nu)$, για κάθε φυσικό ν.

22. Να αποδειχθεί ότι $42 \mid (\nu^7 - \nu)$, για κάθε φυσικό ν.

23. Να αποδειχθεί ότι το γινόμενο τεσσάρων διαδοχικών φυσικών είναι πάντα πολλαπλάσιο του 24.

24. Να αποδειχθεί ότι για κάθε φυσικό ν, ο αριθμός $1492^\nu - 1770^\nu - 1863^\nu + 2141^\nu$ είναι πολλαπλάσιο του 1946.

25. Για κάθε ακέραιο $\alpha \geq 3$, να αποδείξετε ότι $360 \mid \alpha^2(\alpha^2 - 1)(\alpha^2 - 4)$.

26. Να αποδείξετε ότι για κάθε φυσικό ν το κλάσμα

$$\frac{21\nu + 4}{14\nu + 3}$$

    είναι ανάγωγο. (1η ΔΜΟ, 1959, Βουκουρέστι).

27. Έστω α, β, γ ακέραιοι, πρώτοι μεταξύ τους ανά δύο, με α, γ περιττούς και $\alpha^2 + \beta^2 = \gamma^2$. Να αποδείξετε ότι οι αριθμοί $\beta + \gamma$, $\gamma - \beta$ είναι τέλεια τετράγωνα.

1.4 Γραμμική Διοφαντική Εξίσωση

Ας θεωρήσουμε δύο ακεραίους αριθμούς α και β. Γνωρίζουμε ότι υπάρχουν ακέραιοι κ και λ τέτοιοι ώστε

$$\kappa\alpha + \lambda\beta = (\alpha, \beta).$$

Η αντίστροφη διαδικασία προσδιορισμού του Μ.Κ.Δ. των α, β οδηγεί στην εύρεση κατάλληλων κ, λ που ικανοποιούν την προηγούμενη σχέση.
Η γενική μορφή μίας τέτοιας εξίσωσης είναι η $\alpha x + \beta y = \gamma$, όπου α, β και γ είναι γνωστοί ακέραιοι αριθμοί και x, y είναι άγνωστοι ακέραιοι. Η εξίσωση αυτή είναι γνωστή ως γραμμική Διοφαντική εξίσωση.
Για παράδειγμα η εξίσωση $3x + 5y = 4$ έχει λύση το ζεύγος $(3, -1)$, διότι $3 \cdot 3 + 5 \cdot (-1) = 4$. Αντίθετα η εξίσωση $2x + 20y = 1$ δεν έχει λύση, γιατί για κάθε επιλογή του ζεύγους (x, y) το αριστερό μέρος της είναι άρτιος ενώ το δεξί μέρος της είναι περιττός.
Ας δούμε λοιπόν πότε η γραμμική Διοφαντική εξίσωση είναι επιλύσιμη.

Θεώρημα 1.4.1
Η γραμμική Διοφαντική εξίσωση $\alpha x + \beta y = \gamma$ έχει λύση αν και μόνο αν ο $\delta = (\alpha, \beta)$ διαιρεί τον ακέραιο γ.

Απόδειξη.
Ας υποθέσουμε ότι η εξίσωση $\alpha x + \beta y = \gamma$ έχει λύση (x_0, y_0), δηλαδή ισχύει ότι

$$\alpha x_0 + \beta y_0 = \gamma.$$

Θέτουμε $\alpha = \kappa\delta$ και $\beta = \lambda\delta$, όπου κ, λ ακέραιοι. Έτσι έχουμε ότι

$$\gamma = \alpha x_0 + \beta y_0 = \delta(\kappa x_0 + \lambda y_0),$$

όπου ο αριθμός $\kappa x_0 + \lambda y_0$ είναι ακέραιος, οπότε $\delta \mid \gamma$.
Αντίστροφα, ας θεωρήσουμε ότι $\delta \mid \gamma$, οπότε $\gamma = \delta \cdot \mu$, όπου μ ακέραιος. Από το Θεώρημα 1.3.4 γνωρίζουμε ότι υπάρχουν ακέραιοι κ, λ τέτοιοι ώστε:

$$\kappa\alpha + \lambda\beta = (\alpha, \beta) = \delta \quad \text{ή}$$

$$\alpha(\kappa\mu) + \beta(\lambda\mu) = \delta\mu = \gamma.$$

Άρα η εξίσωση $\alpha x + \beta y = \gamma$ έχει λύση $x_0 = \kappa\mu$, $y_0 = \lambda\mu$.

Μια ιδιότητα της γραμμικής Διοφαντικής εξίσωσης είναι ότι οι λύσεις της, αν υπάρχουν, είναι άπειρες και ανήκουν στην ίδια κλάση ισοϋπόλοιπων ακεραίων.

Θεώρημα 1.4.2
Αν (x_0, y_0) είναι μια λύση της εξίσωσης $ax + \beta y = \gamma$ και $\delta = (\alpha, \beta)$, τότε όλες οι λύσεις της είναι της μορφής:

$$x = x_0 + \left(\frac{\beta}{\delta}\right) t \text{ και } y = y_0 - \left(\frac{\alpha}{\delta}\right) t,$$

όπου $t \in \mathbf{Z}$.

Απόδειξη.
Έστω ότι η εξίσωση $ax + \beta y = \gamma$ έχει μια γνωστή λύση (x_0, y_0). Αν υποθέσουμε πως (x, y) είναι μια άλλη λύση, τότε

$$\alpha x_0 + \beta y_0 = \gamma = \alpha x^{'} + \beta y^{'} \ ,$$

το οποίο είναι ισοδύναμο με

$$\alpha(x^{'} - x_0) = \beta(y_0 - y^{'}).$$

Διαιρώντας με τον $\delta = (\alpha, \beta)$, παίρνουμε ότι

$$\varkappa(x^{'} - x_0) = \lambda(y_o - y^{'}) \ ,$$

όπου οι $\varkappa = \frac{\alpha}{\delta}$ και $\lambda = \frac{\beta}{\delta}$ είναι σχετικά πρώτοι. Επομένως έχουμε $\varkappa \mid \lambda(y_0 - y^{'})$ και $(\varkappa, \lambda) = 1$, οπότε το Θεώρημα 1.3.9, έχουμε ότι $\varkappa \mid (y_0 - y^{'})$. Δηλαδή, υπάρχει ακέραιος t τέτοιος ώστε $y_0 - y^{'} = \varkappa t$. Όμοια αποδεικνύεται ότι $x^{'} - x_0 = \lambda t$ κι έτσι καταλήγουμε στους τύπους:

$$x^{'} = x_0 + \lambda t = x_0 + \left(\frac{\beta}{\delta}\right) t$$

$$y^{'} = y_0 - \varkappa t = y_0 - \left(\frac{\alpha}{\delta}\right) t.$$

Παρατήρηση
Εύκολα μπορεί κανείς να παρατηρήσει ότι αν $(\alpha, \beta) = 1$ και η $(x_0\ ,\ y_0)$ είναι μια λύση της γραμμικής Διοφαντικής εξίσωσης, τότε όλες οι λύσεις της είναι της μορφής:

$$x = x_0 + \beta t \quad \text{και} \quad y = y_0 - \alpha t$$

για κάθε ακέραιο t.

Η επίλυση μιας γραμμικής διοφαντικής εξίσωσης ανάγεται στον προσδιορισμό μιας αρχικής της λύσης (x_0, y_0). Η αντίστροφη διαδικασία του αλγορίθμου του Ευκλείδη δίνει τον τρόπο προσδιορισμού μιας τέτοιας λύσης. Αν $\delta = (\alpha, \beta)$, τότε μπόρουμε να βρούμε ακέραιους κ, λ ώστε

$$\kappa\alpha + \lambda\beta = \delta.$$

Υποθέτουμε ότι $\delta \mid \gamma$ (για να υπάρχει λύση) δηλαδή $\gamma = \delta\mu$, για κάποιον ακέραιο μ. Άρα $\mu \cdot \kappa \cdot \alpha + \mu \cdot \lambda \cdot \beta = \mu \cdot \delta = \gamma$, δηλαδή μία λύση της αρχικής εξίσωσης είναι η

$$x_0 = \mu\kappa\ ,\ \ y_0 = \mu\lambda,$$

οπότε η γενική λύση είναι η

$$x = \mu\kappa + \left(\frac{\beta}{\delta}\right) t\ ,\ \ y = \mu\lambda - \left(\frac{\alpha}{\delta}\right) t\ ,\ \ \text{όπου } t \in \mathbf{Z}.$$

Εφαρμογές 1.4

1. Να υπολογισθεί ο μέγιστος κοινός διαιρέτης των αριθμών 172 και 20. Στη συνέχεια να λυθεί η γραμμική Διοφαντική εξίσωση $172x + 20y = 1000$.

Λύση.
Με την βοήθεια του αλγόριθμου του Ευκλείδη υπολογίζουμε τον (172,20),

$$\begin{aligned} 172 &= 8 \cdot 20 + 12 \\ 20 &= 1 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \\ 8 &= 2 \cdot 4. \end{aligned}$$

Άρα $(172, 20) = 4$ και προφανώς η εξίσωση $172x + 20y = 1000$ έχει λύση, διότι $4 \mid 1000$.
Ακολουθώντας την αντίστροφη διαδικασία του αλγόριθμου του Ευκλείδη έχουμε:

$$\begin{aligned} 4 &= 12 - 8 \\ 4 &= 12 - (20 - 12) \\ 4 &= 2 \cdot 12 - 20 \\ 4 &= 2(172 - 8 \cdot 20) - 20 \\ 4 &= 2 \cdot 172 + (-17) \cdot 20. \end{aligned}$$

Άρα $4 = 2 \cdot 172 + (-17) \cdot 20$ και πολλαπλασιάζοντας με 250 προκύπτει ότι

$$172 \cdot 500 + 20 \cdot (-4250) = 1000.$$

Επομένως μια λύση της Διοφαντικής εξίσωσης είναι $x_0 = 500$, $y_0 = -4250$ και σύμφωνα με το Θεώρημα 1.4.2, όλες οι λύσεις της είναι της μορφής:

$$x = 500 + \left(\frac{20}{4}\right) t = 500 + 5t$$

$$y = -4250 - \left(\frac{172}{4}\right) t = -4250 - 43t,$$

όπου $t \in \mathbf{Z}$.

2. Να υπολογισθούν οι φυσικοί αριθμοί οι οποίοι διαιρούμενοι με τον 11 αφήνουν υπόλοιπο 6 και διαιρούμενοι με τον 5 αφήνουν υπόλοιπο 2.

Λύση.
Έστω ένας φυσικός ν τέτοιος ώστε ν=11κ+6 και ν=5λ+2. Τότε

$$11x + 6 = 5\lambda + 2 \text{ ή } 5\lambda - 11x = 4$$

και καταλήγουμε σε μια Διοφαντική εξίσωση η οποία έχει λύση, διότι $(-11, 5) = 1$ και $1 \mid 4$. Εκφράζουμε τον μέγιστο κοινό διαιρέτη $(-11, 5) = 1$ ως γραμμικό συνδυασμό των -11 και 5, με την βοήθεια του αλγόριθμου του Ευκλείδη:

$$\begin{aligned} -11 &= (-3) \cdot 5 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 4 \cdot 1. \end{aligned}$$

Ακολουθώντας την αντίστροφη διαδικασία έχουμε

$$1 = (-2) \cdot 5 + (-1)(-11).$$

Πολλαπλασιάζοντας επί 4 προκύπτει

$$5 \cdot (-8) - 11 \cdot (-4) = 4$$

και μια λύση της Διοφαντικής εξίσωσης είναι

$$\lambda_0 = -8, x_0 = -4.$$

Επομένως, όλες οι λύσεις της είναι της μορφής

$$\begin{aligned} \lambda &= -8 + (-11)t = -11t - 8 \\ x &= -4 - 5t = -5t - 4, \end{aligned}$$

όπου $t \in Z$ και ο φυσικός ν γράφεται $\nu = -55t - 38$. Επειδή πρέπει $\nu > 0$ έχουμε $-55t - 38 > 0$ ή $t < -38/35$ και επειδή t ακέραιος $\nu = -55t - 38$ με $t \leq -1$ ή $\nu = 55t - 38$, $t \in \mathbf{Z}, t \geq 1$.

3. Ένας κουμπαράς περιέχει κέρματα των 50 και 100 δραχμών συνολικού ποσού 1100 δραχμών. Να υπολογίσετε όλους τους δυνατούς συνδυασμούς κερμάτων που μπορούμε να έχουμε.

Λύση.
Αν ορίσουμε x το πλήθος των κερμάτων των 50 δραχμών και y το πλήθος των κερμάτων των 100 δραχμών έχουμε την γραμμική Διοφαντική εξίσωση

$$50x + 100y = 1100.$$

Προφανώς (50,100)=50 και $50 \mid 1100$, οπότε η εξίσωση έχει λύση. Επιπλέον παρατηρούμε ότι

$$50(-1) + 100 \cdot 1 = 50$$

και πολλαπλασιάζοντας με τον αριθμό 22 έχουμε ότι

$$50(-22) + 100 \cdot 22 = 1100,$$

οπότε μια λύση της γραμμικής Διοφαντικής εξίσωσης είναι $x_0 = -22$ και $y_0 = 22$. Από το Θεώρημα 1.4.2, όλες οι λύσεις της είναι της μορφής:

$$\begin{aligned} x &= -22 + \left(\tfrac{100}{50}\right) t &&= -22 + 2t \\ y &= 22 - \left(\tfrac{50}{50}\right) t &&= 22 - t, \end{aligned}$$

όπου $t \in \mathbf{Z}$. Επιπλέον οι αριθμοί x και y είναι μη αρνητικοί, οπότε $-22 + 2t \geq 0$ και $22 - t \geq 0$, δηλαδή $22 \geq t \geq 11$.
Επομένως όλοι οι δυνατοί συνδυασμοί είναι

$$x = 2t - 22 \text{ και } y = 22 - t,$$

όπου $t = 11, 12, \ldots, 22$.

4. Να υπολογισθούν τα κλάσματα, στα οποία αν προσθέσουμε τον αριθμό 3 στον αριθμητή και τον 4 στον παρονομαστή τους γίνονται ίσα με το 6/11.

Λύση.
Έστω x/y ένα κλάσμα, τέτοιο ώστε $\frac{x+3}{y+4} = \frac{6}{11}$.
Τότε έχουμε την Διοφαντική εξίσωση $11x - 6y = -9$, η οποία έχει λύση αφού $(11, -6) = 1$ και $1 \mid (-9)$. Με τη βοήθεια του αλγορίθμου του Ευκλείδη γράφουμε τον $(11, -6) = 1$ ως γραμμικό συνδυασμό των 11 και -6:

$$\begin{aligned} 11 &= (-1) \cdot (-6) + 5 \\ -6 &= (-2) \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \\ 4 &= 1 \cdot 4. \end{aligned}$$

Ακολουθώντας την αντίστροφη διαδικασία έχουμε

$$1 = (-1) \cdot 11 + (-2)(-6).$$

Πολλαπλασιάζοντας επί (-9) προκύπτει ότι

$$11 \cdot 9 - 6 \cdot 18 = -9$$

και μια προφανής λύση της Διοφαντικής εξίσωσης είναι η

$$x_0 = 9 \text{ και } y_0 = 18.$$

Σύμφωνα με το Θεώρημα 1.4.2 όλες οι λύσεις της είναι της μορφής

$$\begin{aligned} x &= 9 + (-6) \cdot t = 9 - 6 \cdot t \\ y &= 18 - 11 \cdot t, \end{aligned}$$

όπου $t \in \mathbf{Z}$. Αν αντικαταστήσουμε τις τιμές αυτές στο κλάσμα έχουμε

$$\frac{x+3}{y+4} = \frac{12-6t}{22-11t} = \frac{6(2-t)}{11(2-t)} = \frac{6}{11}, \text{ αν } t \neq 2.$$

Για $t = 2$ το κλάσμα είναι το $\frac{x}{y} = \frac{3}{4}$ οπότε έχουμε $\frac{x+3}{y+4} = \frac{6}{8}$. Άρα τα ζητούμενα κλάσματα είναι της μορφής

$$\frac{x}{y} = \frac{9-6t}{18-11t},$$

όπου $t \in \mathbf{Z}$, $t \neq 2$.

Ασκήσεις 1.4

Α' Ομάδα

1. Να υπολογισθεί ο μέγιστος κοινός διαιρέτης των αριθμών 1819 και 3587. Κατόπιν να βρεθούν ακέραιοι x και y τέτοιοι ώστε να ισχύει $x \cdot 1819 + y \cdot 3587 = (1819, 3587)$.

2. Να λυθούν οι παρακάτω γραμμικές Διοφαντικές εξισώσεις:

   (i) $56x + 72y = 40$

   (ii) $221x + 91y = 117$

   (iii) $54x + 21y = 906$

   (iv) $158x - 57y = 7$.

3. Να λυθούν οι παρακάτω γραμμικές Διοφαντικές εξισώσεις:

   (i) $97x + 129y = 1$

   (ii) $91x - 98y = 13$

   (iii) $12x - 57y = 2$.

4. Να βρεθεί ένας αριθμός με υπόλοιπο 16 όταν διαιρεθεί με τον 39 και 27 όταν διαιρεθεί με τον 56.

5. Να αποδειχθεί ότι οι παρακάτω εξισώσεις δεν έχουν θετικές ακέραιες λύσεις:

   (i) $7x + 15y = -10$

   (ii) $3x + 15y = 16$

   (iii) $8x + 6y = 10$

6. Να βρεθούν όλοι οι ακέραιοι x, ώστε το πηλίκο $(9 - 7x) : 4$ να είναι πολλαπλάσιο του 3.

7. Έστω δύο φυσικοί α, β και ο μέγιστος κοινός διαιρέτης τους $\delta = (\alpha, \beta)$. Να αποδείξετε ότι αν $\delta = \kappa\alpha + \lambda\beta$ τότε οι αριθμοί κ, λ δεν είναι μοναδικοί.

Β' Ομάδα

8. Σε έναν συνοικιακό κινηματογράφο το εισιτήριο κοστίζει 1800 δραχμές για τους ενήλικες και 750 δραχμές για τα παιδιά. Ένα βράδυ, το σύνολο των εισπράξεων είναι 90.000 δραχμές. Πόσα εισιτήρια κόπηκαν αν γνωρίζουμε ότι οι ενήλικες θεατές ήταν περισσότεροι από τα παιδιά;

9. Να βρείτε δύο κλάσματα με παρανομαστές 5 και 7 που έχουν άθροισμα $26/35$.

10. Αν οι ακέραιοι x και y είναι πολλαπλάσια του 5, να λυθεί η εξίσωση $3x + 4y = 50$.

11. Να υπολογισθούν οι ακέραιες λύσεις της εξίσωσης:
$(3x^2 + 2y - 4)^2) = (2x + y - 5)^2$.

12. Να βρεθούν όλα τα ζεύγη φυσικών λ, κ με $\lambda > 1$, ώστε η εξίσωση

$$(\sqrt{\lambda} - 1)x^2 + 2\sqrt{\mu}x - 3(\sqrt{\lambda} + 1) = 0$$

να έχει μία διπλή ρίζα.

13. Να υπολογισθούν οι ακέραιες λύσεις της εξίσωσης:
$y^2 - 6x^2 + xy - y + 17x - 12 = 0$.

14. Να υπολογίσετε τον μεγαλύτερο ακέραιο γ για τον οποίο η γραμμική Διοφαντική εξίσωση $5x + 7y = \gamma$ έχει 9 ακριβώς θετικές λύσεις.

15. Έχουμε 24 κέρματα των 5, 10 και 20 δραχμών συνολικού ποσού 200 δραχμών. Πόσους δυνατούς συνδυασμούς μπορούμε να έχουμε;

1.5 Ελάχιστο Κοινό Πολλαπλάσιο

Έστω δύο φυσικοί αριθμοί α και β. Θεωρούμε τις ακολουθίες $\alpha, 2\alpha, 3\alpha, \ldots$ και $\beta, 2\beta, 3\beta, \ldots$ και στην προσπάθεια εύρεσης του μικροτέρου κοινού όρου τους, ορίζουμε **κοινό πολλαπλάσιο** των α, β κάθε ακέραιο μ τέτοιον ώστε $\alpha \mid \mu$ και $\beta \mid \mu$. Οι αριθμοί α και β έχουν άπειρα κοινά πολλαπλάσια, ένα από τα οποία είναι το γινόμενο $\alpha\beta$. Το μικρότερο από τα θετικά κοινά πολλαπλάσια των α και β ονομάζεται **ελάχιστο κοινό πολλαπλάσιο** (Ε.Κ.Π) των α, β και συμβολίζεται $\mu = [\alpha, \beta]$. Ο ορισμός προφανώς γενικεύεται για α, β ακέραιους. Οι ιδιότητες του Ε.Κ.Π. εκφράζονται από τις ακόλουθες προτάσεις:

Πρόταση 1.5.1
Αν α και β δύο ακέραιοι, τότε:
(i) $[\alpha, \beta] = [\beta, \alpha]$, $[\alpha, 1] = |\alpha|$ και $[\alpha, 0] = 0$.
(ii) Αν $\alpha \mid \beta$, $\alpha \neq 0$ τότε $[\alpha, \beta] = |\beta|$.
(iii) Αν μ είναι ένα κοινό πολλαπλάσιο των α και β με $\alpha \neq 0$, $\beta \neq 0$, τότε $[\alpha, \beta] \mid \mu$.

Σχόλιο
Παρατηρούμε ότι σε αντίθεση με τον Μ.Κ.Δ. όπου ο (0,0) δεν ορίζεται έχουμε $[0, 0] = 0$.

Πρόταση 1.5.2
Έστω α, β και γ τρεις μη μηδενικοί ακέραιοι, με $\gamma > 0$. Τότε ισχύει:
(i) $[\gamma\alpha, \gamma\beta] = \gamma[\alpha, \beta]$.
(ii) Αν $\gamma \mid \alpha$ και $\gamma \mid \beta$, τότε $[\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}] = \frac{1}{\gamma}[\alpha, \beta]$.

Απόδειξη.
(i) Εφόσον το $[\gamma\alpha, \gamma\beta]$ είναι πολλαπλάσιο του γ, γράφεται $[\gamma\alpha, \gamma\beta] = \gamma \cdot \mu_1$. Συμβολίζοντας το ελάχιστο κοινό πολλαπλάσιο των α και β με $\mu_2 = [\alpha, \beta]$ παρατηρούμε ότι $\gamma\alpha \mid \gamma\mu_2$, $\gamma\beta \mid \gamma\mu_2$, $\gamma\alpha \mid \gamma\mu_1$, $\gamma\beta \mid \gamma\mu_2$, οπότε $\gamma\mu_1 \mid \gamma\mu_2$ από την Πρόταση 1.5.1(iii), άρα $\mu_1 \mid \mu_2$. Όμως $\gamma\alpha \mid \gamma\mu_1$ και $\gamma\beta \mid \gamma\mu_1$, άρα $\alpha \mid \mu_1$, $\beta \mid \mu_1$ και $\mu_2 \mid \mu_1$. Άρα $\mu_1 = \mu_2$, δηλαδή $[\gamma\alpha, \gamma\beta] = \gamma[\alpha, \beta]$.
(ii) Αμεσα από το (i) έχουμε $[\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}] = \frac{\gamma}{\gamma}[\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}] = \frac{1}{\gamma}[\frac{\gamma\alpha}{\gamma}, \frac{\gamma\beta}{\gamma}] = \frac{1}{\gamma}[\alpha, \beta]$.
Αν λοιπόν ψάχνουμε το ελάχιστο κοινό πολλαπλάσιο δύο ακεραίων α, β και γνωρίζουμε έναν κοινό τους διαιρέτη δ, τότε αρκεί να βρούμε το

$[\frac{\alpha}{\delta}, \frac{\beta}{\delta}]$. Ας θεωρήσουμε για παράδειγμα τους αριθμούς 36 και 48 οι οποίοι έχουν κοινό διαιρέτη τον 12. Τότε ισχύει $[36, 48] = [3 \cdot 12, 4 \cdot 12] = 12[3, 4] = 12 \cdot 12 = 144$.

Πρόταση 1.5.3
Αν οι α, β είναι δύο φυσικοί αριθμοί τότε $[\alpha, \beta] = \alpha\beta$ αν και μόνο αν οι α, β είναι πρώτοι μεταξύ τους.

Απόδειξη.
Ας υποθέσουμε ότι για τους α, β ισχύει $[\alpha, \beta] = \alpha\beta$, ενώ $(\alpha, \beta) = \delta > 1$. Τότε υπάρχουν φυσικοί $\varkappa$ και λ, τέτοιοι ώστε $\alpha = \varkappa\delta$ και $\beta = \lambda\delta$, με $(\varkappa, \lambda) = 1$. Επομένως $[\alpha, \beta] = \delta\,[\varkappa, \lambda]$ από την Πρόταση 1.5.2(i).
Άρα $\delta[\varkappa, \lambda]{=}(\delta\varkappa)(\delta\lambda)$ ή $[\varkappa, \lambda] = \delta\varkappa\lambda$, με $\delta > 1$, το οποίο είναι άτοπο, αφού $[\varkappa, \lambda] \leq \varkappa\lambda$. Επομένως οι αριθμοί α και β είναι σχετικά πρώτοι.

Αντίστροφα, ας δεχθούμε ότι οι α και β είναι σχετικά πρώτοι, ενώ $[\alpha, \beta] \neq \alpha\beta$. Τότε από την Πρόταση 1.5.2(iii) υπάρχει ακέραιος $\varkappa > 1$, τέτοιος ώστε $\alpha\beta = \varkappa[\alpha, \beta]$ δηλαδή $\alpha\beta = [\varkappa\alpha, \varkappa\beta]$. Επομένως $\varkappa\alpha \mid \alpha\beta$ και $\varkappa\beta \mid \alpha\beta$ ή $\varkappa \mid \beta$ και $\varkappa \mid \alpha$. Δηλαδή $\varkappa \mid (\alpha, \beta)$, το οποίο είναι άτοπο, αφού $(\alpha, \beta){=}1$. Άρα αν οι α και β είναι σχετικά πρώτοι, τότε ισχύει $[\alpha, \beta] = \alpha\beta$.

Στην απόδειξη της Πρότασης 1.5.3 είναι φανερή η άμεση σχέση του μέγιστου κοινού διαιρέτη και του ελάχιστου κοινού πολλαπλάσιου δύο σχετικά πρώτων φυσικών αριθμών. Η σχέση αυτή γενικεύεται στην παρακάτω πρόταση, η οποία ανάγει τον προσδιορισμό του Ε.Κ.Π.στην εύρεση του Μ.Κ.Δ.

Πρόταση 1.5.4
Αν α και β είναι δύο φυσικοί αριθμοί, τότε ισχύει ότι
$[\alpha, \beta] \cdot (\alpha, \beta) = \alpha\beta$.

Απόδειξη.
Αν $\delta = (\alpha, \beta)$, τότε οι ακέραιοι $\frac{\alpha}{\delta}$ και $\frac{\beta}{\delta}$ ειναι σχετικά πρώτοι, λόγω του Πορίσματος 1.3.8. Επομένως από την Πρόταση 1.5.3 έχουμε ότι $\left[\frac{\alpha}{\delta}, \frac{\beta}{\delta}\right] = \frac{\alpha}{\delta}\frac{\beta}{\delta}$ ή $\frac{1}{\delta}[\alpha, \beta] = \frac{1}{\delta^2}\alpha\beta$. Άρα $\delta[\alpha, \beta] = \alpha\beta$.

Από την παραπάνω πρόταση προκύπτει ότι αν α και β είναι δύο ακέραιοι αριθμοί, όχι και οι δύο μηδέν, τότε:

$$[\alpha, \beta](\alpha, \beta) = |\alpha\beta| \,.$$

Εφαρμογές 1.5

1. Αν α και β είναι δύο φυσικοί αριθμοί, τότε $(\alpha, \beta) = [\alpha, \beta]$ αν και μόνο αν $\alpha = \beta$.

   Απόδειξη.
   Από τη σχέση $(\alpha, \beta) = [\alpha, \beta]$ έχουμε ότι $\alpha \mid (\alpha, \beta)$, δηλαδή $\alpha \mid \beta$.
   Όμοια και $\beta \mid \alpha$, συνεπώς $\alpha = \beta$.
   Αντίστροφα, αν $\alpha = \beta$, τότε $(\alpha, \alpha) = \alpha = [\alpha, \alpha]$.

2. Βρείτε το ελάχιστο κοινό πολλαπλάσιο των αριθμών 143 και 227.

   Λύση.
   Αρχικά υπολογίζουμε τον μέγιστο κοινό διαιρέτη δ=(143, 227) με τον Αλγόριθμο του Ευκλείδη :

$$\begin{aligned} 227 &= 1 \cdot 143 + 84 \\ 143 &= 1 \cdot 84 + 59 \\ 84 &= 1 \cdot 59 + 25 \\ 59 &= 2 \cdot 25 + 9 \\ 25 &= 2 \cdot 9 + 7 \\ 9 &= 1 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

   Επομένως (143, 227)=1 και από την Πρόταση 1.5.4 καταλήγουμε ότι $[143, 227] = 143 \cdot 227 = 32461$.

3. Βρείτε ακεραίους x και y τέτοιους ώστε $(165, 418) = 165x + 418y$. Κατόπιν να υπολογίσετε το [165, 418].

   Λύση.
   Χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη έχουμε

$$\begin{aligned} 418 &= 2 \cdot 165 + 88 \\ 165 &= 1 \cdot 88 + 77 \\ 88 &= 1 \cdot 77 + 11 \\ 77 &= 7 \cdot 11. \end{aligned}$$

   Άρα (165, 418)=11 και ως γνωστόν η εξίσωση $165x + 418y$=11 έχει λύση.

Ακολουθώντας τα αντίστροφα βήματα του αλγορίθμου του Ευκλείδη έχουμε:

$$\begin{aligned} 11 &= 88 - 77 \\ &= 88 - (165 - 88) \\ &= 2 \cdot 88 - 165 \\ &= 2(418 - 2 \cdot 165) - 165. \end{aligned}$$

Άρα $11 = 2 \cdot 418 - 5 \cdot 165$, δηλαδή $x = -5$ και $y = 2$.
Τέλος το ελάχιστο κοινό πολλαπλάσιο των αριθμών 165 και 418 είναι

$$[165, 418] = \frac{165 \cdot 418}{(165,418)} = \frac{165 \cdot 418}{11}$$

$$= 15 \cdot 418 = 6270.$$

4. Αν α, β είναι θετικοί ακέραιοι, να αποδειχθεί ότι:
$(\alpha, \beta) = (\alpha + \beta, [\alpha, \beta])$.

Απόδειξη.
Αν $\delta_1 = (\alpha, \beta)$, τότε $\delta_1 \mid \alpha$ και $\delta_1 \mid \beta$. Επομένως $\delta_1 \mid (\alpha + \beta)$, $\delta_1 \mid [\alpha, \beta]$ και $\delta_1 \leq (\alpha + \beta, [\alpha, \beta])$.
Αν $\delta_2 = (\alpha + \beta, [\alpha + \beta])$, τότε $\delta_2 \mid (\alpha + \beta)$ και $\delta_2 \mid [\alpha, \beta]$.

Δηλαδή $\delta_2 \mid \frac{\alpha \cdot \beta}{(\alpha,\beta)}$, όπου οι αριθμοί α και $\frac{\beta}{(\alpha,\beta)}$ είναι πρώτοι μεταξύ τους. Επομένως, $\delta_2 \mid \alpha$ ή $\delta_2 \mid \frac{\beta}{(\alpha,\beta)}$. Και στις δύο περιπτώσεις, έχουμε ότι $\delta_2 \mid \alpha$ και $\delta_2 \mid \beta$. Άρα $\delta_2 \leq \delta_1$ και προφανώς $\delta_1 = \delta_2$.

Ασκήσεις 1.5

Α' Ομάδα

1. Να ολοκληρωθεί η απόδειξη της Πρότασης 1.5.1.

2. Βρείτε το ελάχιστο κοινό πολλαπλάσιο των αριθμών :
(i) 106 και 654, (ii) 120 και 84,
(iii) 54 και 162, (iv) 6 και 1024.

3. Να αποδειχθεί ότι για κάθε φυσικό $\nu > 1$ ισχύει:
(i) $[\nu,\ \nu+1] = \nu(\nu+1)$ και (ii) $[2\nu-1,\ 2\nu+1] = (2\nu-1)(2\nu+1)$.

4. Βρείτε τους φυσικούς α και β $(\alpha \leq \beta)$ με $(\alpha, \beta) = 10$ και $[\alpha, \beta] = 100$.

5. Να υπολογισθεί ο μικρότερος φυσικός Ν, ο οποίος διαιρούμενος με τους αριθμούς 2, 3, 4, ..., 10 αφήνει υπόλοιπα 1, 2, 3, ..., 9 αντίστοιχα.

1.6 Πρώτοι Αριθμοί

Γνωρίζουμε ότι κάθε φυσικός αριθμός διαιρείται με τον εαυτό του και την μονάδα. Αν επιπλέον δεν διαιρείται με κανένα άλλο φυσικό αριθμό τότε ονομάζεται **πρώτος**. Ένας πρώτος αριθμός είναι σχετικά πρώτος με όλους τους μικρότερούς του φυσικούς.

Αν ένας φυσικός δεν είναι πρώτος, τότε έχει τουλάχιστον ένα διαιρέτη διαφορετικό του 1 μικρότερό του και ονομάζεται **σύνθετος**. Έτσι λοιπόν, οι αριθμοί 2, 3, 5, 7 και 11 είναι πρώτοι, ενώ οι 4, 6, 8, 9 και 10 είναι σύνθετοι. Επιπλέον, ο μοναδικός άρτιος πρώτος φυσικός είναι ο 2, ο οποίος διαιρεί όλους τους άρτιους. Η μονάδα δεν θεωρείται ούτε πρώτος, ούτε σύνθετος αριθμός. Έτσι το σύνολο $\mathbf{N}$ των φυσικών αριθμών διαμερίζεται σε τρία σύνολα, το σύνολο των πρώτων αριθμών, το σύνολο των σύνθετων αριθμών και το μονοσύνολο $\{1\}$.
Επίσης έχουμε ότι αν α είναι ένας ακέραιος και p ένας πρώτος αριθμός με $p < \alpha$, τότε $(p, \alpha)=1$ αν και μόνο αν ο p δεν διαιρεί τον α.

Πρόταση 1.6.1
Αν α και β είναι δύο ακέραιοι και p ένας πρώτος αριθμός τέτοιος ώστε $p \mid \alpha\beta$, τότε $p \mid \alpha$ ή $p \mid \beta$.
Απόδειξη.
Αν $p \mid \alpha$, η πρόταση ισχύει.
Αν ο p δεν διαιρεί τον α, τότε $(p,\alpha)=1$ και από το Θεώρημα 1.3.9 έχουμε ότι $p \mid \beta$.

Το πρώτο ερώτημα που τίθεται είναι το πώς μπορούμε να εξακριβώσουμε αν ένας δοσμένος αριθμός είναι πρώτος. Το κριτήριο που ακολουθεί, χωρίς να είναι το καλύτερο δυνατό (βλ. Κεφ. 4) μειώνει σημαντικά το πλήθος των δυνατών πρώτων παραγόντων που χρειάζεται να ελέγξουμε.

Πρόταση 1.6.2 (Κριτήριο Ρίζας)
Κάθε σύνθετος αριθμός $\alpha > 1$ έχει έναν τουλάχιστον πρώτο παράγοντα $p \leq \sqrt{\alpha}$.
Απόδειξη.
Θεωρούμε p το μικρότερο διαιρέτη του α με $p > 1$. Τότε ο p είναι πρώτος αριθμός, διαφορετικά θα γραφόταν ως $p = \beta\gamma$, με $\beta, \gamma > 1$ και

οι αριθμοί β και γ θα ήταν διαιρέτες του α μικρότεροι από τον p, άτοπο. Επιπλέον ο αριθμός α γράφεται $\alpha = p\beta$, με $1 < p \leq \beta < \alpha$ και από τη σχέση $p^2 \leq p\beta = \alpha$ είναι φανερό ότι $p \leq \sqrt{\alpha}$.

Από την παραπάνω πρόταση προκύπτει άμεσα ότι :

Παρατήρηση
Αν ένας φυσικός αριθμός α δεν έχει πρώτο διαιρέτη μικρότερο ή ίσο του $\sqrt{\alpha}$, τότε είναι πρώτος.

Το ακόλουθο βασικό θεώρημα της Θεωρίας των Αριθμών αναδεικνύει τον ρόλο των πρώτων ως "δομικά" στοιχεία των φυσικών ως προς την πράξη του πολλαπλασιασμού.

Θεώρημα 1.6.3 (Θεμελιώδες Θεώρημα της Αριθμητικής)
Κάθε ακέραιος αριθμός $\alpha > 1$ μπορεί να γραφεί ως γινόμενο πρώτων παραγόντων κατά μοναδικό τρόπο, αν δε λάβουμε υπόψη τη σειρά των παραγόντων.

Απόδειξη.

Στην περίπτωση που ο α είναι πρώτος αριθμός, τότε γράφεται ως γινόμενο πρώτων με έναν παράγοντα και το θεώρημα προφανώς ισχύει.
Αν ο αριθμός α είναι σύνθετος, τότε από την Πρόταση 1.6.2 γράφεται στη μορφή: $\alpha = p_1 \cdot \beta_1$, όπου ο p_1 είναι ένας πρώτος αριθμός μικρότερος του $\sqrt{\alpha}$. Αν ο β_1 είναι πρώτος, τότε η παραγοντοποίηση σταματά. Διαφορετικά γράφεται $\beta_1 = p_2 \cdot \beta_2$, όπου ο p_2 είναι πρώτος αριθμός μικρότερος του $\sqrt{\beta_1}$. Συνεχίζοντας τη διαδικασία αυτή, έπειτα από $\kappa < \frac{\alpha}{2}$ βήματα , βρίσκουμε κ (όχι απαραίτητα διακεκριμένους ανά δύο) πρώτους αριθμούς $p_1, p_2, \ldots, p_\kappa$, τέτοιους ώστε $\alpha = p_1 p_2 \ldots p_\kappa$. Μένει τώρα να αποδείξουμε τη μοναδικότητα αυτών των πρώτων παραγόντων. Ας υποθέσουμε πως ο α γράφεται

$$\alpha = p_1 p_2 \cdots p_\kappa = q_1 q_2 \cdots q_\mu.$$

Επειδή $p_1 \mid \alpha$ και

$$p_1 \mid q_1 q_2 \cdots q_\mu$$

από την Πρόταση 1.6.1 προκύπτει ότι $p_1 = q_j$, για κάποιο $j \in \{1, 2, \ldots, \mu\}$. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι $j = 1$ και $p_1 = q_1$. Έτσι έχουμε $p_2 p_3 \ldots p_\kappa = q_2 q_3 \ldots q_\mu$.

Επαναλαμβάνουμε την ίδια διαδικασία έως ότου εξαντληθεί το ένα

από τα δύο μέλη της παραπάνω ισότητας. Έτσι καταλήγουμε στο ότι $\kappa = \mu$ και όλοι οι πρώτοι παράγοντες $p_1, p_2, \ldots, p_\kappa$ αντιστοιχούν σε ίσους αριθμούς από τους παράγοντες $q_1, q_2, \ldots, q_k$. Άρα η γραφή

$$\alpha = p_1 p_2 \ldots p_\kappa$$

είναι μοναδική αν δε λάβουμε υπόψη την σειρά των παραγόντων.

Στην παραγοντοποίηση ενός φυσικού αριθμού α σε γινόμενο πρώτων παραγόντων, κάποιοι παράγοντες μπορεί να εμφανίζονται περισσότερες από μια φορές. Αν ο πρώτος p_j εμφανίζεται α_j φορές ως παράγοντας, τότε ο α γράφεται

$$\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$$

με $p_1 < p_2 < \ldots < p_\kappa$ θετικούς πρώτους. Η γραφή αυτή του φυσικού αριθμού α ονομάζεται **κανονική μορφή** του α.

Η γραφή ενός φυσικού αριθμού στην κανονική του μορφή βοηθά στη λύση πολλών προβλημάτων. Για παράδειγμα, αν θέλουμε να περιγράψουμε το μέγιστο κοινό διαιρέτη δ ή το ελάχιστο κοινό πολλαπλάσιο μ δύο φυσικών αριθμών α και β, μπορούμε να τους εκφράσουμε ως γινόμενο πρώτων παραγόντων

$$\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa} \quad \text{και} \quad \beta = p_1^{\beta_1} p_2^{\beta_2} \ldots p_\kappa^{\beta_\nu},$$

όπου $\alpha_j \geq 0$ και $\beta_j \geq 0$ για $j = 1, 2, \ldots$ και να γράψουμε το μέγιστο κοινό διαιρέτη στην κανονική μορφή του:

$$\delta = (\alpha, \beta) = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \ldots p_\kappa^{\min(\alpha_\kappa, \beta_\kappa)}$$

και όμοια έχουμε την κανονική μορφή του ελάχιστου κοινού πολλαπλασίου:

$$\mu = [\alpha, \beta] = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \ldots p_\kappa^{\max(\alpha_\kappa, \beta_\kappa)}.$$

Επιπλέον είναι φανερό ότι

$$\begin{aligned}(\alpha, \beta)[\alpha, \beta] &= p_1^{\min(\alpha_1, \beta_1) + \max(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2) + \max(\alpha_2, \beta_2)} \ldots \\ &\qquad \ldots p_\kappa^{\min(\alpha_\kappa, \beta_\kappa) + \max(\alpha_\kappa, \beta_\kappa)} \\ &= p_1^{\alpha_1 + \beta_1} p_2^{\alpha_2 + \beta_2} \ldots p_\kappa^{\alpha_\kappa + \beta_\kappa} \\ &= \alpha\beta\end{aligned}$$

κι έτσι έχουμε μια δεύτερη απόδειξη της Πρότασης 1.5.4.

Σχόλιο
Με βάση το προηγούμενο θεώρημα κάθε φυσικός α γράφεται $\alpha = 2^{\nu}\beta$ με $\nu \geq 0$ και β είναι ένας περιττός.

Είναι ενδιαφέρον το ότι το πλήθος των πρώτων αριθμών προσδιορίσθηκε πολύ νωρίς.

Θεώρημα 1.6.4 (Ευκλείδης)
Το πλήθος των πρώτων αριθμών είναι άπειρο.

Απόδειξη.
Ας υποθέσουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων $p_1, p_2, \ldots, p_\nu$. Θεωρούμε τον αριθμό

$$N = 1 + p_1 p_2 \cdots p_\nu$$

ο οποίος προφανώς δεν έχει πρώτο διαιρέτη κανένα από τους αριθμούς $p_1, p_2, \ldots, p_\nu$. Άρα ο N είναι ένας πρώτος αριθμός μεγαλύτερος των $p_1, p_2, \ldots, p_\nu$, άτοπο.

Με βάση το Θεμελιώδες Θεώρημα της Αριθμητικής είναι φανερό ότι αν γνωρίζουμε την κατανομή των πρώτων αριθμών στο σύνολο των φυσικών αριθμών **N**, τότε γνωρίζουμε τη δομή των φυσικών , γεγονός που δεν ήταν εφικτό με τις κλάσεις ισοϋπολοίπων. Αξιοσημείωτο είναι το ότι το πρόβλημα του προσδιορισμού της ακριβούς κατανομής των πρώτων στο N παραμένει ακόμη ανοιχτό παρά τα σημαντικά αποτελέσματα πολλών ερευνητών (βλ. Κεφ. 4).
Αν και το πλήθος των πρώτων είναι άπειρο, κανείς δε γνωρίζει την ακριβή κατανομή των πρώτων, δηλαδή έναν τύπο που να μας δίνει όλους τους πρώτους. Πολλές συναρτήσεις δίνουν πρώτους αριθμούς για ένα πλήθος τιμών της μεταβλητής x, αλλά αργά ή γρήγορα δίνουν σύνθετους.
Χαρακτηριστικό παράδειγμα (αποδίδεται στον Euler) είναι η συνάρτηση $f(x) = x^2 + x + 41$, η οποία δίνει πρώτους για $x = 0, 1, 2, \ldots, 38, 39$ ενώ $f(40) = 1681 = 41^2$.
Επιπλέον, επειδή $f(x-1) = f(-x)$ η f δίνει επίσης πρώτους για $x = -1, -2, ..., -40$.
Έτσι, η $g(x) = f(x-40) = x^2 - 79x + 1601$ δίνει πρώτους για 80 διαδοχικούς αριθμούς $x = 0, 1, 2, \ldots, 79$ ενώ για $x = 80$ δίνει σύνθετο.
Ο μεγαλύτερος πρώτος αριθμός που έχει προσδιορισθεί (Ιανουάριος 1998)

είναι ο

$$2^{3021377} - 1$$

και έχει 909526 ψηφία.
Μελετώντας μεγάλους αριθμούς παρατηρούμε ότι οι πρώτοι γίνονται όλο και πιο σπάνιοι, και μάλιστα σύμφωνα με το ακόλουθο θεώρημα μπορούμε να βρούμε 2 διαδοχικούς πρώτους που να απέχουν περισσότερο από οποιονδήποτε δοσμένο αριθμό.

Θεώρημα 1.6.5
Για κάθε φυσικό ν, υπάρχουν ν διαδοχικοί σύνθετοι αριθμοί.
Απόδειξη.
Για έναν τυχαίο φυσικό ν θεωρούμε τους αριθμούς

$$(\nu+1)!+2, (\nu+1)!+3, \ldots, (\nu+1)!+\nu+1$$

όπου $\kappa! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \kappa$ είναι το γνωστό κ-παραγοντικό.
Οι αριθμοί αυτοί είναι ν στο πλήθος και όλοι τους σύνθετοι, γιατί για κάθε $\mu = 2, 3, \ldots, \nu+1$ ο μ διαιρεί τον $(\nu+1)!+\mu$.

Ένα από τα άλυτα προβλήματα που αφορούν τους πρώτους αριθμούς είναι, αν υπάρχουν άπειροι "δίδυμοι πρώτοι", δηλαδή ζευγάρια πρώτων της μορφής $p, p+2$.
Το ίδιο ισχύει για τις τριάδες πρώτων της μορφής $\{p, p+2, p+6\}$ και $\{p, p+4, p+6\}$.
Είναι όμως βέβαιο ότι δεν υπάρχουν τριάδες πρώτων της μορφής $p, p+2, p+4$, αφού κάποιος από τους τρεις θα διαιρείται με τον 3.

Εφαρμογές 1.6

1. Να βρεθούν όλοι οι πρώτοι της μορφής $x^3 - 1$.

   Λύση.
   Κάθε φυσικός $\alpha = x^3 - 1$ γράφεται ως $\alpha = (x-1)(x^2+x+1)$.
   Άρα ο α είναι πρώτος αν και μόνο αν $x - 1 = 1$ ή $x = 2$.
   Δηλαδή, ο μοναδικός πρώτος της μορφής $x^3 - 1$ είναι ο $\alpha = 2^3 - 1 = 8 - 1 = 7$.

2. Αν $p \neq 2, 5$ είναι ένας πρώτος, τότε ο αριθμός 10 διαιρεί τον $p^2 - 1$ ή τον $p^2 + 1$.

   Αποδειξη.
   Εφόσον ο p είναι πρώτος αριθμός διάφορος των 2 και 5, θα γράφεται σε μια από τις μορφές $5x + 1$, $5x + 2$, $5x + 3$ ή $5x + 4$.
   Αν $p = 5x + 1$, τότε ο $p^2 - 1 = 25x^2 + 10x$ είναι ταυτόχρονα άρτιος και πολλαπλάσιο του 5, άρα $10 \mid (p^2 - 1)$.
   Όμοια, αποδεικνύονται και οι υπόλοιπες περιπτώσεις.

3. Να αποδειχθεί ότι δεν υπάρχουν διακεκριμένοι πρώτοι αριθμοί p, q, r, s τέτοιοι ώστε $p \cdot s - q \cdot r = 0$.

   Απόδειξη.
   Αν $p \cdot s = q \cdot r$, τότε είναι προφανές ότι $p | qr$ και προκύπτει ότι $p = q$ ή $p = r$, *άτοπο*.
   Άρα δεν υπάρχει τετράδα διακεκριμένων πρώτων p, q, r, s τέτοιοι ώστε $ps - qr = 0$.

4. Να αποδείξετε ότι κάθε αριθμός της μορφής $\nu^4 + 4$ με $\nu > 1$ και ν όχι πολλαπλάσιο του 5, είναι σύνθετος.

   Απόδειξη.
   Γνωρίζουμε ότι $\nu^2 = 5x \pm 1$, άρα ο αριθμός $\nu^4 + 4$ γράφεται

$$\begin{aligned} \nu^4 + 4 &= 25x^2 \pm 10x + 1 + 4 \\ &= 5(5x^2 \pm 2x + 1) \end{aligned}$$

   και προφανώς είναι σύνθετος.

5. Να αποδειχθεί ότι δεν υπάρχει τριάδα διαδοχικών περιττών που να είναι πρώτοι, εκτός από την τριάδα 3, 5, 7.

   Απόδειξη.
   Έστω ν, $\nu+2$, $\nu+4$ διαδοχικοί περιττοί. Γνωρίζουμε ότι αν $\nu > 3$, τότε τουλάχιστον ένας από αυτούς διαιρείται με τον 3.
   Άρα η μόνη τριάδα διαδοχικών περιττών πρώτων είναι η $(3, 5, 7)$.

6. Αν ένας πρώτος αριθμός p διαιρεί τον α^ν τότε $p^\nu \mid \alpha^\nu$.

   Απόδειξη.
   Αν $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa}$ η κανονική μορφή του α, τότε έχουμε

   $$\alpha^\nu = p_1^{\nu\alpha_1} p_2^{\nu\alpha_2} \dots p_\kappa^{\nu\alpha_\kappa}$$

   και αφού $p \mid \alpha^\nu$ συμπεραίνουμε ότι $p = p_j$ για κάποιο φυσικό j. Επομένως ο α^ν έχει παράγοντα της μορφής $p^{\nu\alpha_j}$, όπου $\alpha_j \geq 1$ οπότε $p^\nu \mid \alpha^\nu$.

7. Αν μ και ν είναι δύο διαδοχικοί περιττοί πρώτοι αριθμοί, να αποδειχθεί ότι το άθροισμά τους έχει τουλάχιστον τρεις πρώτους παράγοντες, όχι υποχρεωτικά διακεχριμένους.

   Απόδειξη.
   Αφού οι μ και ν είναι περιττοί, υπάρχει ένας φυσικός κ τέτοιος ώστε $\nu = \mu + 2\kappa$. Επομένως $\mu + \nu = \mu + \mu + 2\kappa = 2(\mu + \kappa)$.
   Επιπλέον ο $\mu + \kappa$ βρίσκεται μεταξύ των μ και ν, άρα δεν είναι πρώτος, οπότε έχει τουλάχιστον δύο πρώτους διαιρέτες, όχι υποχρεωτικά διακεχριμένους.
   Επομένως και το άθροισμα $\mu + \nu$ έχει τρεις τουλάχιστον πρώτους παράγοντες, όχι υποχρεωτικά διακεχριμένους.

8. Ο μεγαλύτερος γνωστός πρώτος είναι ένας αριθμός του Mersenne, δηλαδή ένας αριθμός της μορφής $2^\kappa - 1$. Να αποδείξετε ότι, αν ο αριθμός $2^\kappa - 1$ είναι πρώτος, τότε και ο κ είναι πρώτος. Ισχύει το αντίστροφο;

   Απόδειξη.
   Έστω ότι ο κ είναι σύνθετος, δηλαδή $\kappa = \alpha\beta$, με $\alpha, \beta \geq 2$. Τότε

   $$2^\kappa - 1 = 2^{\alpha\beta} - 1^\beta = (2^\alpha - 1)(2^{\alpha(\beta-1)} + 2^{\alpha(\beta-2)} + \dots + 1)$$

δηλαδή ο $2^x - 1$ είναι σύνθετος, άτοπο.
Άρα αν ο $2^x - 1$ είναι πρώτος τότε και ο x είναι πρώτος. Το αντίστροφο δεν ισχύει, αφού $2^{11} - 1 = 2047 = 23 \cdot 89$.

9. Υπάρχουν φυσικοί μ και ν, τέτοιοι ώστε ο αριθμός $N = \mu^4 + 4\nu^4$ να είναι πρώτος;

Λύση.
Ο αριθμός N γράφεται

$$\begin{aligned} N &= \mu^4 + 4\nu^4 \\ &= (\mu^2)^2 + 4\mu^2\nu^2 - 4\mu^2\nu^2 + (2\nu^2)^2 \\ &= (\mu^2 + 2\nu^2)^2 - (2\mu\nu)^2 \\ &= (\mu^2 - 2\mu\nu + 2\nu^2)(\mu^2 + 2\mu\nu + 2\nu^2). \end{aligned}$$

Αν N είναι πρώτος θα πρέπει ο μικρότερος παράγοντάς του να είναι ίσος με τον 1. Δηλαδή, θέλουμε

$$\begin{aligned} \mu^2 - 2\mu\nu + 2\nu^2 &= 1 \quad \text{ή} \\ \mu^2 - 2\mu\nu + \nu^2 + \nu^2 &= 1 \quad \text{ή} \\ (\mu - \nu)^2 + \nu^2 &= 1. \end{aligned}$$

Άρα η μοναδική λύση είναι $\mu = \nu = 1$.

10. Αν p και q είναι δύο διακεχριμένοι πρώτοι αριθμοί τέτοιοι ώστε $p \cdot q \mid \nu^2$, τότε να αποδειχθεί ότι $p \cdot q \mid \nu$.

Απόδειξη.
Επειδή $p \cdot q \mid \nu^2$ θα πρέπει $p \mid \nu^2$ και $q \mid \nu^2$, οπότε $p \mid \nu$ και $q \mid \nu$.
Άρα $p \cdot q \mid \nu$.

11. Κάθε φυσικός της μορφής $3x+2$ έχει έναν πρώτο διαιρέτη της ίδιας μορφής.

Απόδειξη.
Έστω ένας τυχαίος φυσικός $\alpha = 3\nu + 2$ με $\nu \geq 1$. Αν ο α είναι πρώτος τότε έχει πρώτο διαιρέτη της μορφής $3x+2$ τον εαυτό του. Αν ο α είναι σύνθετος τότε έχει πρώτους διαιρέτες της μορφής $3x+1$ ή $3x+2$. Αποκλείεται όλοι οι πρώτοι διαιρέτες του αριθμού α να είναι της μορφής $3x+1$, διότι τότε και ο α θα ήταν της ίδια μορφής, άτοπο. Επομένως υπάρχει διαιρέτης του α, της μορφής $3x+2$.

12. Έστω Σ ένα τυχαίο σύνολο $\nu+1$ φυσικών αριθμών μικρότερων ή ίσων του 2ν. Να αποδειχθεί ότι υπάρχουν $\alpha, \beta \in \Sigma$ τέτοιοι ώστε $\alpha \mid \beta$.

Απόδειξη.
Κάθε φυσικός μ γράφεται στη μορφή $\mu = 2^{x}\lambda$, όπου ο λ είναι περιττός. Αν λοιπόν το σύνολο Σ είναι :

$$\Sigma = \{\mu_i \in N : i = 1, 2, 3, \ldots, \nu+1\}$$

τότε όλα τα στοιχεία του γράφονται στη μορφή:

$$\mu_i = 2^{x_i}\lambda_i, i = 1, 2, \ldots, \nu, \nu+1.$$

Οι $\nu+1$ περιττοί αριθμοί $\lambda_1, \lambda_2, \ldots, \lambda_{\nu+1}$ περιέχονται στο σύνολο $\{1, 3, 5, \ldots, 2\nu-1\}$, το οποίο περιέχει ν ακριβώς στοιχεία. Άρα δύο τουλάχιστον από αυτούς τους περιττούς ταυτίζονται, έστω οι $\lambda_\rho = \lambda_\tau = \gamma$. Συμπεραίνουμε, λοιπόν, ότι οι αριθμοί $\mu_\tau = 2^{x_\tau}\lambda_\tau = 2^{x_\tau}\gamma$ και $\mu_\rho = 2^{x_\rho}\lambda_\rho = 2^{x_\rho}\gamma$ είναι ο ένας πολλαπλάσιο του άλλου.

13. Να αποδείξετε ότι το πλήθος των πρώτων αριθμών της μορφής $4\nu+3$ είναι άπειρο.

Απόδειξη.
Ας θεωρήσουμε ότι υπάρχει πεπερασμένο πλήθος πρώτων αριθμών της μορφής $4x+3$ και p_0 είναι ο μεγαλύτερος από αυτούς. Αν β είναι το γινόμενο όλων των πρώτων από 2 ως και p_0, τότε ο αριθμός $\alpha = 2\beta - 1$ είναι της μορφής $\alpha = 4\gamma - 1 = 4(\gamma-1)+3$ και δεν έχει πρώτο διαιρέτη μικρότερο του p_0+1. Επιπλέον, αποκλείεται όλοι οι διαιρέτες του α να είναι της μορφής $4\nu+1$, αφού στην περίπτωση αυτή και ο α θα ήταν της ίδιας μορφής. Επομένως, ο αριθμός α είναι πρώτος ή έχει διαιρέτη δ της μορφής $4\nu+3$ με $\delta > p_0$. Και στις δύο περιπτώσεις καταλήγουμε σε άτοπο.

Ασκήσεις 1.6

Α' Ομάδα

1. Αν p_1 και p_2 είναι δύο πρώτοι αριθμοί, να αποδειχθεί ότι $(p_1, p_2) \neq 1$ αν και μόνο αν $p_1 \equiv p_2$.

2. Αν p_1, p_2 και p είναι πρώτοι αριθμοί τέτοιοι ώστε $p \mid p_1 p_2$, να αποδειχθεί ότι $p = p_1$ ή $p = p_2$.

3. Αν $p_1, p_2, \ldots, p_\kappa$ και p είναι πρώτοι αριθμοί τέτοιοι ώστε $p \mid p_1 \ldots p_\kappa$, να αποδειχθεί ότι $p = p_j$, για κάποιο $j \in \{1, 2, \ldots, \kappa\}$.

4. Να αποδειχθεί ότι κάθε πρώτος της μορφής $3\kappa + 1$ γράφεται στη μορφή $6\kappa + 1$.

5. Έστω $\kappa > 1$ ο μικρότερος φυσικός που διαιρεί έναν φυσικό αριθμό ν. Να αποδειχθεί ότι ο κ είναι πρώτος.

6. Βρείτε την κανονική μορφή των αριθμών 1234, 10140 και 36000.

7. Υπολογίστε τον μέγιστο κοινό διαιρέτη των αριθμών 5247000 και 189280.

8. Αν α και β είναι δύο φυσικοί αριθμοί με κανονική μορφή $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\nu^{\alpha_\nu}$ και $\beta = p_1^{\beta_1} p_2^{\beta_2} \ldots p_\kappa^{\beta_\kappa}$, να αποδείξετε την κανονική μορφή του (α, β) και $[\alpha, \beta]$.

9. Να αποδείξετε ότι κάθε πρώτος αριθμός είναι της μορφής $3\nu + 1$ ή $6\nu - 1$.

10. Να αποδείξετε ότι κάθε φυσικός μεγαλύτερος του 11 γράφεται ως άθροισμα δύο σύνθετων αριθμών.

11. Αν οι αριθμοί p, $p + 4$ είναι πρώτοι, με $p > 3$, να αποδείξετε ότι $9 \mid (3p + 6)$.

12. Έστω α, β, κ τρεις φυσικοί αριθμοί τέτοιοι ώστε $\alpha^\kappa \mid \beta^\kappa$. Να αποδειχθεί ότι $\alpha \mid \beta$.

13. Έστω τέσσερεις φυσικοί αριθμοί α, β, μ, ν, με $\mu \leq \nu$ και $\alpha^\nu \mid \beta^\mu$. Να αποδειχθεί ότι $\alpha \mid \beta$.

14. Αν ο φυσικός αριθμός ν δεν είναι της μορφής $\nu = 6x + 3$, να αποδειχθεί ότι ο $N = \nu^2 + 2^\nu$ είναι σύνθετος.

15. Έστω ένας φυσικός αριθμός $\nu \geq 2$. Να αποδειχθεί ότι ο $N = \nu^4 + 4^\nu$ είναι σύνθετος.

16. Βρείτε όλους τους πρώτους παράγοντες του αριθμού 50!.

17. Βρείτε τον ελάχιστο φυσικό αριθμό ν, τέτοιον ώστε ο $945 \cdot \nu$ να είναι τέλειο τετράγωνο ακεραίου.

Β' Ομάδα

18. Να αποδείξετε ότι αν ένας από τους αριθμούς,

$$2^\nu - 1, \ 2^\nu + 1$$

είναι πρώτος τότε ο αλλος είναι σύνθετος, όπου $\nu \geq 2$.

19. Έστω α, β, γ, δ φυσικοί αριθμοί με $\alpha\beta = \gamma\delta$. Να αποδείξετε ότι ο αριθμός $\alpha + \beta + \gamma + \delta$ είναι σύνθετος.

20. Να αποδειχθεί ότι ο μοναδικός πρώτος αριθμός της μορφής $p = x^3 + 1$ είναι ο αριθμός 2.

21. Έστω p πρώτος και α, β φυσικοί τέτοιοι ώστε $(\alpha, p^2) = p$ και $(\beta, p^4) = p^2$. Να υπολογίσετε τους αριθμούς $(\alpha\beta, p^5)$, $(\alpha + \beta, p^2)$, $(\alpha - \beta, p^5)$, $(p\alpha - \beta, p^5)$.

22. Αν p και $p + 2$ είναι δύο διαδοχικοί πρώτοι με $p > 3$, τότε να αποδειχθεί ότι $6 \mid (p + 1)$.

23. Να εξετάσετε αν υπάρχουν πρώτοι της μορφής: $p = \alpha^4 - \beta^4$, με $\alpha > \beta$ φυσικούς αριθμούς.

24. Να αποδειχθεί ότι δεν υπάρχουν διαδοχικοί θετικοί ακέραιοι, οι οποίοι να είναι τέλεια τετράγωνα ακεραίων.

25. Να βρεθούν όλοι οι φυσικοί αριθμοί οι οποίοι μπορούν να γραφούν ως άθροισμα ή διαφορά δύο πρώτων και αφήνουν υπόλοιπο 9 διαιρούμενοι με το 154.

26. Να αποδειχθεί ότι το τετράγωνο κάθε πρώτου αριθμού p μεγαλύτερου του 3 είναι της μορφής $p^2 = 12\nu + 1$.

27. Έστω ένας άρτιος φυσικός $\nu \geq 2$. Να εξετάσετε αν ο αριθμός $\mathrm{N}= \underbrace{111\ldots1}_{\nu-\psi\eta\phi\iota\alpha}$ είναι πρώτος.

28. Έστω ν ακέραιος μεγαλύτερος ή ίσος του 2. Αν ο αριθμός $N = \underbrace{111\ldots1}_{\nu-\psi\eta\phi\iota\alpha}$ είναι πρώτος, να αποδείξετε ότι και ο ν είναι πρώτος.

29. Έστω δύο φυσικοί αριθμοί α, β και ένας πρώτος p. Αν $p \mid \alpha\beta$ και $p \mid (\alpha + \beta)$, να αποδειχθεί ότι $p \mid (\alpha, \beta)$.

30. Αν α και β είναι δύο φυσικοί αριθμοί, πρώτοι μεταξύ τους, να αποδειχθεί ότι $(\alpha + \beta,\ \alpha \cdot \beta) = 1$.

31. Έστω p ένας πρώτος αριθμός και α, ν δύο θετικοί ακέραιοι τέτοιοι ώστε $p \mid \alpha^\nu$. Να αποδειχθεί ότι $p \mid \alpha$.

32. Έστω θετικός ακέραιος ν και p ένας πρώτος αριθμός. Να εξετασθεί πότε οι αριθμοί ν και $\nu + p$ είναι τέλεια τετράγωνα ακεραίων.

33. Αν ο αριθμός $x^\nu + 1$, με $x > 1$, είναι πρώτος, να αποδείξετε ότι ο x είναι άρτιος και ο ν είναι μία δύναμη του 2.

34. Έστω μ, ν και δ τρεις φυσικοί αριθμοί με $(\mu, \nu) = 1$ και $\delta \mid \mu\nu$. Να αποδειχθεί ότι ο φυσικός δ μπορεί να γραφεί στη μορφή $\delta = p \cdot q$, όπου $p \mid \mu$ και $q \mid \nu$.

35. Αν ο φυσικός $p \geq 5$ είναι πρώτος, τότε να αποδείξετε ότι ο $p^2 + 2$ είναι σύνθετος.

36. Να αποδείξετε ότι για κάθε σύνθετο $\nu > 4$, ο αριθμός ν διαιρεί τον $(\nu - 1)!$.

37. Να αποδειχθεί ότι δεν υπάρχει πολυώνυμο $P(x)$ με ακέραιους συντελεστές που η αριθμητική του τιμή να είναι πρώτος αριθμός για κάθε φυσικό x.

38. Να αποδειχθεί ότι υπάρχουν άπειροι πρώτοι αριθμοί της μορφής $6x + 5$.

39. Αν ένας φυσικός αριθμός είναι της μορφής $4x+3$ ή $6x+5$, τότε έχει έναν πρώτο διαιρέτη της ίδιας μορφής.

40. Έστω τρεις φυσικοί αριθμοί α, β, γ με $\alpha \mid \beta\gamma$ και $(\alpha, \beta) = \delta$. Να αποδειχθεί ότι $\alpha \mid \delta\gamma$.

41. Αν p και q είναι δύο πρώτοι αριθμοί, με $p \geq q \geq 5$, τότε να αποδείξετε ότι $24 \mid p^2 - q^2$.

42. Να επαληθευθεί ότι το πολυώνυμο

$$Q(x) = x^2 - 79x + 1601$$

δίνει αριθμητική τιμή πρώτο αριθμό, για $x = 0, 1, 2, \ldots, 79$ αλλά όχι για $x = 80$.

1.7 Πλήθος και Άθροισμα Διαιρετών

Χρησιμοποιώντας τη γραφή των φυσικών αριθμών στην κανονική τους μορφή είναι πλέον δυνατός ο υπολογισμός του πλήθους και του αθροίσματος των διαιρετών τους.

Ας θεωρήσουμε έναν φυσικό αριθμό α στην κανονική του μορφή

$$\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa}$$

όπου οι $p_1, p_2, \dots, p_\kappa$ είναι πρώτοι αριθμοί μεγαλύτεροι του 1 με $p_1 < p_2 < \dots < p_\kappa$, και οι $\alpha_1, \alpha_2, \dots, \alpha_\kappa$ είναι κατάλληλοι φυσικοί. Κάθε φυσικός παράγοντας δ του α είναι της μορφής:

$$\delta = p_1^{\beta_1} p_2^{\beta_2} \dots p_\kappa^{\beta_\kappa}$$

όπου $0 \leq \beta_i \leq \alpha_i$ για κάθε $i = 1, 2, \dots, \kappa$.

Ο πρώτος p_i μπορεί να εμφανισθεί στην κανονική μορφή του δ, αν συμπεριλάβουμε και το 1, κατά α_i+1 τρόπους:

$$p_i^0 = 1 \text{ ή } p_i \text{ ή } p_i^2 \text{ ή } \dots \text{ ή } p_i^{\alpha_i}.$$

Επομένως οι πρώτοι αριθμοί $p_1, p_2, \dots, p_\kappa$ εμφανίζονται σε όλους τους παράγοντες του α κατά $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_\kappa + 1)$ τρόπους. Δηλαδή ο φυσικός α έχει συνολικά

$$\delta(\alpha) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_\kappa + 1)$$

διαφορετικούς φυσικούς παράγοντες.

Για παράδειγμα, ο αριθμός $48 = 2^4 3^1$ έχει $\delta(48) = (4+1)(1+1) = 10$ διαιρέτες. Πράγματι οι διαιρέτες του 48 είναι οι 1, 2, 3, 4, 6, 8, 12, 16, 24 και 48. Η συνάρτηση $\delta(\alpha)$ που εκφράζει το πλήθος των διαιρετών του φυσικού αριθμού α, είναι μία πολλαπλασιαστική συνάρτηση, όπως φαίνεται από την παρακάτω πρόταση.

Πρόταση 1.7.1
Αν δύο φυσικοί α και β είναι πρώτοι μεταξύ τους, τότε το πλήθος των φυσικών διαιρετών του γινομένου $\alpha\beta$ είναι $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$.

Απόδειξη.
Εφόσον $(\alpha, \beta) = 1$, οι φυσικοί α και β δεν θα έχουν κοινούς πρώτους παράγοντες στην κανονική τους μορφή. Κάθε φυσικός διαιρέτης δ του γινομένου $\alpha\beta$ θα γράφεται $\delta = \delta_1 \cdot \delta_2$, όπου $\delta_1 \mid \alpha$ και $\delta_2 \mid \beta$. Για τον διαιρέτη δ_1 έχουμε $\delta(\alpha)$ επιλογές και για τον δ_2 έχουμε $\delta(\beta)$ επιλογές. Επομένως καταλήγουμε στο ότι $\delta(\alpha\beta) = \delta(\alpha)\delta(\beta)$.

Αλλες συναρτήσεις με παρόμοιες ιδιότητες είναι η $\sigma(\alpha)$, που ορίζεται ως άθροισμα των φυσικών διαιρετών του α, και η συνάρτηση Euler $\varphi(\alpha)$, που ορίζεται ως το πλήθος των αριθμών του συνόλου $\{1, 2, \ldots, \alpha - 1\}$ που είναι σχετικά πρώτοι με τον α. Τη συνάρτηση Euler θα μελετήσουμε στο 2ο και 3ο Κεφάλαιο.

Θεώρημα 1.7.2
Αν δύο φυσικοί α και β είναι σχετικά πρώτοι τότε $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$.

Απόδειξη.
Ας θεωρήσουμε ότι $\gamma_1 = 1, \gamma_2, \gamma_3, \ldots, \gamma_\kappa = \alpha$ είναι όλοι οι φυσικοί διαιρέτες του α και $\delta_1 = 1, \delta_2, \ldots, \delta_\mu = \beta$ είναι όλοι οι φυσικοί διαιρέτες του β. Αφού $(\alpha, \beta)=1$, κάθε φυσικός διαιρέτης του γινομένου $\alpha\beta$ θα είναι της μορφής $\gamma_i\delta_j$ με $i \in \{1, 2, \ldots, k\}$ και $j \in \{1, 2, \ldots, \mu\}$. Επομένως,

$$\begin{aligned}
\sigma(\alpha\beta) &= \gamma_1\delta_1 + \gamma_1\delta_2 + \ldots + \gamma_2\delta_1 + \gamma_2\delta_2 + \ldots + \gamma_\kappa\delta_{\mu-1} + \gamma_\kappa\delta_\mu \\
&= \gamma_1(\delta_1 + \delta_2 + \ldots + \delta_\mu) + \ldots + \gamma_\kappa(\delta_1 + \delta_2 + \ldots + \delta_\mu) \\
&= (\delta_1 + \delta_2 + \ldots + \delta_\mu)(\gamma_1 + \gamma_2 + \ldots + \gamma_\kappa) \\
&= \sigma(\beta)\sigma(\alpha).
\end{aligned}$$

Για το υπολογισμό του αθροίσματος των διαιρετών ενός φυσικού αριθμού αρκεί—λόγω του ότι είναι πολλαπλασιαστική συνάρτηση—να υπολογίσουμε την τιμή του σε δυνάμεις πρώτων.

Πρόταση 1.7.3
Αν p και α είναι δύο φυσικοί αριθμοί και ο p είναι πρώτος, τότε

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}.$$

Απόδειξη.
Εφόσον ο p είναι πρώτος, οι μόνοι διαιρέτες του αριθμού p^α είναι οι $1, p, p^2, \ldots, p^{\alpha-1}, p^\alpha$.
Άρα $\sigma(p^\alpha) = 1 + p + p^2 + \ldots + p^\alpha = (p^{\alpha+1} - 1)/(p - 1)$.

Χρησιμοποιώντας την προηγούμενη πρόταση, τώρα είμαστε σε θέση να υπολογίσουμε το άθροισμα των διαιρετών ενός φυσικού αριθμού αν γνωρίζουμε την κανονική του μορφή.

Θεώρημα 1.7.4

Αν ο α είναι φυσικός αριθμός με κανονική μορφή $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa}$, τότε

$$\sigma(\alpha) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\dots\left(\frac{p_\kappa^{\alpha_\kappa+1}-1}{p_\kappa-1}\right).$$

Απόδειξη.

Η απόδειξη είναι άμεση συνέπεια του Θεωρήματος 1.7.2 σε συνδυασμό με την Πρόταση 1.7.3.

Για παράδειγμα, ο αριθμός $48 = 2^4 \cdot 3^1$ έχει άθροισμα διαιρετών:

$$\sigma(48) = \frac{2^{4+1}-1}{2-1} \cdot \frac{3^{1+1}-1}{3-1} = \frac{32-1}{1} \cdot \frac{9-1}{2} = 124$$

και πράγματι 1+2+3+4+6+8+12+16+24+48=124.

Ένα ενδιαφέρον πρόβλημα είναι η εύρεση φυσικών αριθμών που το άθροισμα των διαιρετών τους είναι κάποιας συγκεκριμένης μορφής. Για παράδειγμα το $\sigma(66)$=144 είναι τετράγωνο ακεραίου. Ένας φυσικός αριθμός α ονομάζεται **τέλειος**, όταν ισούται με το άθροισμα όλων των φυσικών διαιρετών του, μικροτέρων του α. Δηλαδή, για κάθε τέλειο αριθμό α ισχύει ότι $\sigma(\alpha) = 2\alpha$.

Μέχρι το 1996 είχαν βρεθεί 35 τέλειοι αριθμοί

$$6, 28, 496, 8128, 33550336, \dots, 2^{1398268}(2^{1398269}-1).$$

Δύο ακόμη μεγαλύτεροι έχουν προσδιορισθεί το 1997 και το 1998 και ελέγχονται.

Και οι 37 παραπάνω αριθμοί είναι άρτιοι, ενώ παραμένει αναπάντητο το ερώτημα αν υπάρχουν περιττοί τέλειοι αριθμοί. Πάντως αν υπάρχει κάποιος περιττός τέλειος, αυτός θα είναι μεγαλύτερος του 10^{300} [Brend,Cohen, Riele, 1991], θα έχει τουλάχιστον 29 πρώτους παράγοντες [Sayers,1988] και ο μεγαλύτερος πρώτος παράγοντας του θα είναι μεγαλύτερος του 500000 [Bradstein, 1982].

Η μορφή των τέλειων άρτιων αριθμών εκφράζεται από το ακόλουθο θεωρήμα.

Θεώρημα 1.7.5
Αν ο α είναι ένας τέλειος άρτιος, τότε υπάρχει φυσικός αριθμός ν, τέτοιος ώστε

$$\alpha = 2^{\nu-1}(2^{\nu}-1)$$

όπου ο $2^{\nu}-1$ είναι πρώτος αριθμός.

Απόδειξη.
Αφού ο α είναι άρτιος θα γράφεται στη μορφή $\alpha = 2^{\nu-1}\beta$, όπου $\nu \geq 2$ και ο β είναι περιττός. Ακόμη, $\sigma(\alpha) = 2\alpha$ ή $\sigma(2^{\nu-1}\beta) = 2^{\nu}\beta$ ή $\sigma(\beta) = \frac{2^{\nu}\beta}{\sigma(2^{\nu-1})}$.
Δηλαδή, έχουμε ότι $\sigma(\beta) = \frac{2^{\nu}\beta}{2^{\nu}-1}$ με $(2^{\nu}, 2^{\nu}-1) = 1$.
Επομένως $(2^{\nu}-1)|\beta$ και $\sigma(\beta) = \beta + \frac{\beta}{2^{\nu}-1}$, όπου ο αριθμός $\frac{\beta}{2^{\nu}-1}$ είναι διαιρέτης του β. Κάτι τέτοιο είναι δυνατό μόνο αν ο αριθμός β είναι πρώτος και $\frac{\beta}{2^{\nu}-1} = 1$. Άρα $\beta = 2^{\nu}-1$, $\alpha = 2^{\nu-1}(2^{\nu}-1)$ και ο $2^{\nu}-1$ είναι πρώτος.

Είδαμε ότι ένας αριθμός ονομάζεται τέλειος αν $\sigma(\nu) = 2\nu$. Ο Ευκλείδης ήξερε ότι ο αριθμός $2^{p-1}(2^p-1)$ είναι τέλειος αν ο 2^p-1 είναι πρώτος. Ωστόσο, ο Erdös απέδειξε ότι υπάρχουν άπειροι φυσικοί, ν τέτοιοι ώστε η εξίσωση $\sigma(x) = 2\nu$ δεν έχει λύση. Στον ακόλουθο πίνακα παρατίθενται οι φυσικοί μικρότεροι του 1000 με την ιδιότητα αυτή:

2	5	52	88	96	120	124	146	162	178	188	206	210
216	238	246	248	262	268	276	288	290	292	304	307	322
324	326	336	342	372	406	408	426	430	448	472	474	498
516	518	520	530	540	553	556	562	576	584	612	624	626
628	658	668	670	714	718	726	732	738	748	750	756	766
768	782	784	792	802	804	818	836	848	852	872	892	894
896	898	902	916	926	936	964	966	976	982	996		

Ανοιχτό ερώτημα παραμένει η κατανομή των αριθμών αυτών στο $\mathbf{N}$.

Εφαρμογές 1.7

1. Να υπολογίσετε τους δ(4950) και σ(4950).

   Λύση.
   Βρίσκουμε αρχικά την κανονική μορφή του αριθμού 4950:

$$4950 = 2^1 \cdot 3^2 \cdot 5^2 \cdot 11^1$$

   Άρα δ(4950)=(1+1)(2+1)(2+1)(1+1)=36 και

$$\begin{aligned} \sigma(4950) &= \tfrac{2^2-1}{2-1} \cdot \tfrac{3^3-1}{3-1} \cdot \tfrac{5^3-1}{5-1} \cdot \tfrac{11^2-1}{11-1} \\ &= \tfrac{3}{1} \cdot \tfrac{26}{2} \cdot \tfrac{124}{4} \cdot \tfrac{120}{10} \\ &= 3 \cdot 13 \cdot 31 \cdot 12 = 14508. \end{aligned}$$

   Εύκολα μπορεί κανείς να παρατηρήσει ότι οι διαιρέτες του 4950 είναι οι 1, 2, 3, 5, 6, 9, 10, 11, 15, 18, 22, 25, 30, 33, 45, 50, 55, 66, 75, 90, 99, 110, 150, 165, 198, 225, 275, 330, 450, 495, 550, 825, 990, 1650, 2475, 4950.

2. Για κάθε φυσικό ν, να αποδείξετε ότι $\delta(\nu) \leq 2\sqrt{\nu}$.

   Απόδειξη.
   Αν $\delta \mid \nu$, τότε ένας από τους παράγοντες δ και $\frac{\nu}{\delta}$ θα είναι μικρότερος ή ίσος του $\sqrt{\nu}$. Επομένως, οι μισοί παράγοντες του ν θα είναι μικρότεροι ή ίσοι του $\sqrt{\nu}$ και προφανώς $\frac{\delta(\nu)}{2} < \sqrt{\nu}$.

3. Για κάθε φυσικό $\nu = 2^{\varkappa-1}$, με $\varkappa \geq 2$, να αποδείξετε ότι $\sigma(\nu) = 2\nu - 1$.

   Απόδειξη.
   Από την Πρόταση 1.7.3 έχουμε ότι $\sigma(\nu) = (2^{(\varkappa-1)+1} - 1)/(2-1) = 2^{\varkappa} - 1$.
   Άρα $\sigma(\nu) = 2 \cdot 2^{\varkappa-1} - 1 = 2\nu - 1$.

4. Να αποδείξετε ότι καμμία δύναμη πρώτου αριθμού δεν είναι τέλειος αριθμός.

   Απόδειξη.
   Για έναν πρώτο αριθμό p κι έναν τυχαίο φυσικό κ, οι παράγοντες του p^κ είναι οι $1, p, p^2, \ldots, p^{\kappa-1}, p^\kappa$. Επομένως

$$1 + p + p^2 + \ldots + p^{\kappa-1} < \underbrace{p^{\kappa-1} + p^{\kappa-1} + \ldots + p^{\kappa-1}}_{p-\text{φορές}}$$

   Άρα $1+p+p^2+\ldots+p^{\kappa-1} < p^\kappa$ και ο αριθμός p^κ δεν είναι τέλειος.

5. Ένας φυσικός αριθμός α είναι πρώτος αν και μόνο αν $\sigma(\alpha) = \alpha+1$.

   Απόδειξη.
   Αν ο αριθμός α είναι πρώτος, τότε οι μοναδικοί φυσικοί διαιρέτες του είναι οι α και 1 και επομένως $\sigma(\alpha) = \alpha + 1$.
   Αντίστροφα, αν $\sigma(\alpha) = \alpha + 1$ και υποθέσουμε ότι ο α δεν είναι πρώτος, τότε θα έχει έναν τουλάχιστον διαιρέτη δ με $1 < \delta < \alpha$ και $\sigma(\alpha) \geq 1 + \delta + \alpha > \alpha + 1$, άτοπο.

6. Ένας φυσικός αριθμός α έχει περιττό πλήθος παραγόντων αν και μόνο αν ο α είναι τέλειο τετράγωνο ακεραίου.

   Απόδειξη.
   Έστω $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ η κανονική μορφή του α. Το πλήθος των παραγόντων $\delta(\alpha) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_\kappa + 1)$ είναι περιττό αν και μόνο αν όλοι οι παράγοντες

$$\alpha_1 + 1, \alpha_2 + 1, \ldots, \alpha_\kappa + 1$$

   είναι περιττοί. Άρα το $\delta(\alpha)$ είναι περιττός αν και μόνο αν οι $\alpha_1, \alpha_2, \ldots, \alpha_\kappa$ είναι άρτιοι, δηλαδή

$$\alpha = (p_1^{\alpha_1/2} p_2^{\alpha_2/2} \ldots p_\kappa^{\alpha_\kappa/2})^2.$$

7. Κάθε άρτιος τέλειος αριθμός λήγει σε 6 ή 8.

Απόδειξη.
Από το Θεώρημα 1.7.5. γνωρίζουμε ότι κάθε τέλειος άρτιος αριθμός α γράφεται στη μορφή

$$\alpha = 2^{\nu-1}(2^{\nu}-1)$$

όπου ο $2^{\nu}-1$ είναι πρώτος. Λόγω της προηγούμενης εφαρμογής, ο ν είναι πρώτος αριθμός. Έτσι έχουμε τρεις περιπτώσεις:

(i) Αν $\nu = 2$, τότε $\alpha = 2(2^2-1) = 6$.

(ii) Αν $\nu = 4x+1$, τότε ο $\alpha = 2^{4x}(2^{4x+1}-1)$, λήγει σε 6, αφού οι αριθμοί $2^{4x} = 16^x$ και $2^{4x+1}-1 = 2\cdot 16^x - 1$, λήγουν σε 6 και 1 αντίστοιχα.

(iii) Αν $\nu = 4x+3$, τότε ο $\alpha = 2^{4x+2}(2^{4x+3}-1)$, λήγει σε 8, αφού οι αριθμοί $2^{4x+2} = 4\cdot 16^x$ και $2^{4x+3}-1 = 8\cdot 16^x - 1$ λήγουν σε 4 και 7 αντίστοιχα.

Ασκήσεις 1.7

Α' Ομάδα

1. Να αποδείξετε ότι οι αριθμοί 120 και 672 είναι τέλειοι.

2. Υπολογίστε το δ(ν) για ν=3655 και 4503. Να αποδείξετε ότι και στις δύο περιπτώσεις ισχύει $\delta(\nu) = \delta(\nu+1) = \delta(\nu+2) = \delta(\nu+3)$.

3. Υπολογίστε το $\sigma(\nu)$ για ν=14, 206 και 957. Να αποδείξετε ότι και στις τρεις περιπτώσεις ισχύει $\sigma(\nu) = \sigma(\nu+1)$.

4. Βρείτε όλους τους φυσικούς αριθμούς που έχουν ακριβώς δύο διαιρέτες.

5. Βρείτε όλους τους φυσικούς που έχουν ακριβώς τρεις διαιρέτες.

6. Να αποδειχθεί ότι δεν υπάρχει φυσικός ν, τέτοιος ώστε σ(ν)=10.

7. Έστω ένας φυσικός ν τέτοιος ώστε το πλήθος $\delta(\nu)$ των διαιρετών του να είναι πρώτος αριθμός. Να αποδειχθεί ότι ο ν είναι δύναμη πρώτου αριθμού.

Β' Ομάδα

8. Βρείτε φυσικό $\nu \leq 70$ με $\delta(\nu) = 12$.

9. Αν $\kappa_1 = 1, \kappa_2, \ldots, \kappa_\nu = \alpha$ είναι όλοι οι παράγοντες του φυσικού αριθμού α, τότε να αποδείξετε ότι $\frac{1}{\kappa_1} + \frac{1}{\kappa_2} + \ldots + \frac{1}{\kappa_\nu} = \frac{\sigma(\alpha)}{\alpha}$. Τι παρατηρείτε αν ο α είναι τέλειος αριθμός;

10. Αν $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ είναι η κανονική μορφή του $\nu > 1$, να αποδείξετε ότι :

$$1 > \frac{\nu}{\sigma(\nu)} > \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_\kappa}\right).$$

11. Αν ο $\nu > 1$ είναι σύνθετος, τότε να αποδείξετε ότι $\sigma(\nu) > \nu + \sqrt{\nu}$.

12. Αν ο $\alpha > 6$ είναι ένας άρτιος τέλειος αριθμός, να αποδείξετε ότι είναι της μορφής α=6κ+1.

13. Βρείτε τα δύο τελευταία ψηφία του τέλειου αριθμού $\nu = 2^{19936}(2^{19937} - 1)$.

14. Να βρεθούν όλοι οι θετικοί ακέραιοι κ για τους οποίους υπάρχει κάποιος θετικός ακέραιος ν τέτοιος ώστε να ισχύει $\delta(\nu^2)/\delta(\nu) = \kappa$. (39η ΔΜΟ, 1998, Taiwan)

Γενικές Ασκήσεις 1ου Κεφαλαίου

1. Να αποδειχθεί ότι κάθε φυσικός αριθμός που δεν είναι δύναμη του 2 γράφεται ως άθροισμα κάποιων διαδοχικών φυσικών.

2. Να αποδειχθεί ότι ο αριθμός $N = 11^{10} - 1$ είναι πολλαπλάσιο του 100.

3. Να αποδείξετε ότι ο αριθμός

$$\frac{\nu^2 + 23}{24}$$

είναι ακέραιος, όταν ο ν δεν είναι πολλαπλάσιο του 2 ή του 3.

4. Να αποδείξετε ότι ο αριθμός

$$\frac{\nu^9 - \nu^3}{54}$$

είναι ακέραιος.

5. Να αποδείξετε ότι ο αριθμός $\underbrace{11\ldots111}_{1997}\ \underbrace{22\ldots2}_{1998}5$ είναι τέλειο τετράγωνο ακεραίου (2η BMON, 1998, Αθήνα).

6. Να υπολογισθεί ο μικρότερος φυσικός κ για τον οποίο $1441 \mid (60^\nu + \kappa \cdot 71^\nu)$ για κάθε περιττό φυσικό ν.

7. Αν μ και ν είναι δύο φυσικοί τέτοιοι ώστε

$$\frac{\mu}{\nu} = 1 + \frac{1}{2} - \frac{2}{3} + \frac{1}{4} + \frac{1}{5} - \frac{2}{6} + \frac{1}{7} + \frac{1}{8} - \frac{2}{9} + \ldots + \frac{1}{478} + \frac{1}{479} - \frac{2}{480}$$

να αποδειχθεί ότι $641 \mid \mu$.

8. Ένας κτηνοτρόφος έχει ένα κοπάδι πρόβατα. Όταν ρωτήθηκε πόσα πρόβατα έχει, απάντησε:
"Εχω περισσότερα από 250 και λιγότερα από 300 ζώα. Οταν τα μετράω ανά 12 περισσεύουν 9 και όταν τα μετράω ανά 16 περισσεύουν 5".
Πόσα πρόβατα έχει συνολικά;

9. Έστω δύο φυσικοί ν, $\alpha > 1$ τέτοιοι ώστε ο αριθμός $\alpha^\nu + 1$ να είναι πρώτος. Να αποδειχθεί ότι ο α είναι άρτιος και ο ν είναι δύναμη του 2.

10. Έστω p ένας περιττός πρώτος και μ, ν δύο φυσικοί τέτοιοι ώστε $p \mid (\mu^p + \nu^p)$. Να αποδειχθεί ότι $p^2 \mid (\mu^p + \nu^p)$.

11. Αν α, β είναι δύο σχετικά πρώτοι ακέραιοι, να υπολογίσετε τον $(\alpha^2 + \beta^2, \alpha + \beta)$.

12. Αν $(\alpha, \beta) = 1$, να αποδειχθεί ότι ο αριθμός $(\alpha^3 + \beta^3, \alpha^2 + \beta^2)$ διαιρεί τον $\alpha - \beta$.

13. Έστω τυχαίοι φυσικοί α, β και ν. Να αποδείξετε ότι $(\alpha, \beta)^\nu = (\alpha^\nu, \beta^\nu)$.

14. Να αποδειχθεί ότι για κάθε τριάδα φυσικών α, β, γ ισχύει ότι

$$(\alpha, \beta\gamma) = (\alpha, (\alpha, \beta)\gamma).$$

15. Αν α, β, γ είναι τρεις ακέραιοι αριθμοί, να αποδειχθεί ότι $[\alpha, \beta] \mid \gamma$ αν και μόνο αν $\alpha \mid \gamma$ και $\beta \mid \gamma$.

16. Έστω τέσσερεις φυσικοί αριθμοί α, β, γ και ν τέτοιοι ώστε $(\alpha, \beta) = 1$ και $\alpha\beta = \gamma^\nu$. Να αποδειχθεί ότι υπάρχουν φυσικοί δ και ε τέτοιοι ώστε $\alpha = \delta^\nu$ και $\beta = \varepsilon^\nu$.

17. Να αποδείξετε ότι ο αριθμός $3^{6\nu} - 2^{6\nu}$ διαιρείται με το 665 για κάθε τιμή του φυσικού ν.

18. Έστω $p > 2$ ένας πρώτος και

$$1 + \frac{1}{2^3} + \frac{1}{3^3} + \ldots + \frac{1}{(p-1)^3} = \frac{\mu}{\nu},$$

όπου μ, ν πρώτοι μεταξύ τους. Να αποδείξετε ότι ο p διαιρεί τον μ.

19. Ονομάζουμε ένα φυσικό αριθμό "ενδιαφέρον", αν μπορεί να γραφεί ως γινόμενο δύο πρώτων αριθμών. Να βρείτε το μέγιστο πλήθος διαδοχικών αριθμών οι οποίοι να είναι όλοι "ενδιαφέροντες".

20. Να αποδείξετε ότι κανένας από τους αριθμούς

$$\alpha_\nu = 2^{2^\nu} + 1$$

όπου $\nu = 0, 1, 2, \ldots$ δεν είναι κύβος ακεραίου.

21. Να βρείτε όλους τους φυσικούς x, y που ικανοποιούν τη σχέση $x^y = y^x$, με $x \neq y$.

22. Έστω $P(x)$ ένα πολυώνυμο με ακέραιους συντελεστές τέτοιο ώστε

$$P(-\nu) < P(\nu) < \nu$$

για κάποιο ακέραιο ν. Να αποδείξετε ότι $P(-\nu) < -\nu$.

23. Για κάθε περιττό αριθμό ν, να αποδείξετε ότι ο αριθμός

$$\nu^{12} - \nu^8 - \nu^4 + 1$$

διαιρείται με το 512.

24. Να αποδείξετε ότι υπάρχουν ακέραιοι φυσικοί α με την ιδιότητα: ο αριθμός $z = \nu^4 + \alpha$ δεν είναι πρώτος για κάθε φυσικό ν.
(11η ΔΜΟ, 1969, Βουκουρέστι)

25. Να βρεθούν όλοι οι φυσικοί αριθμοί $\nu \geq 1$ τέτοιοι ώστε ο $3^{\nu-1} + 5^{\nu-1}$ να διαιρεί τον $3^\nu + 5^\nu$.

26. Να αποδείξετε ότι ο αριθμός $2222^{5555} + 5555^{2222}$ διαιρείται με το 7.

27. Να βρείτε το πλήθος των σχετικά πρώτων αριθμών α, β με $\alpha + \beta = 7250$.

28. Έστω $\delta(\nu)$ το πλήθος των θετικών διαιρετών του φυσικού ν (συμπεριλαμβανομένων του 1 και ν). Να αποδείξετε ότι υπάρχουν άπειροι φυσικοί αριθμοί ν τέτοιοι ώστε ο $\nu/\delta(\nu)$ να είναι ακέραιος.

29. Βρείτε τους φυσικούς αριθμούς των οποίων το άθροισμα των διαιρετών τους είναι περιττός αριθμός.

30. Να προσδιορίσετε το μέγιστο κοινό διαιρέτη $(2^\nu - 1, 2^\mu + 1)$ όπου μ, ν φυσικοί και ν περιττός.

31. Να αποδείξετε ότι δεν υπάρχουν ακέραιοι αριθμοί κ, λ, μ ώστε

$$\kappa^3 + \lambda^2 - \kappa^\mu = 0.$$

32. Έστω H το σύνολο όλων των φυσικών της μορφής $4\kappa + 1$.
Να αποδείξετε ότι:
(α) Αν $\alpha, \beta \in H$ τότε και $\alpha\beta \in H$
(β) Ένας αριθμός $p \in H$ ονομάζεται πρώτος του Hilbert όταν ισχύει ότι:

$$\alpha\nu\ p = \alpha\beta,\ \ (\alpha, \beta \in H)\ \text{τότε}\ \alpha = 1\,,\ \beta = p\ \text{ή}\ \alpha = p\,,\ \beta = 1.$$

Να αποδείξετε ότι κάθε $\nu \in H$ αναλύεται σε γινόμενο πρώτων του Hilbert αλλά όχι με μοναδικό τρόπο.

Κεφάλαιο 2

Αλγεβρικές Ισοτιμίες

Εισαγωγή

Οι ισοτιμίες εισήγαγαν στη Θεωρία Αριθμών αλγεβρική δομή. Υπήρξαν άμεσα φορμαλιστικά αποτελέσματα και η πεποίθηση ότι γνωστά αλγεβρικά συμπεράσματα θα ήταν δυνατό να εφαρμοσθούν στη νέα αυτή αλγεβρική μορφή της Θεωρίας Αριθμών. Παρ' όλο που αυτό δεν έγινε εφικτό, αφήνοντας αναπάντητα τα βασικά ανοιχτά ερωτήματα της Θεωρίας Αριθμών, υπήρξαν σημαντικά επιτεύγματα που επιβεβαίωσαν την εισαγωγή των αλγεβρικών ισοτιμιών στη Θεωρία Αριθμών.

2.1 Ορισμοί-Ιδιότητες

Ορισμός

Έστω α, β, ν ακέραιοι με $\nu > 0$. Θα λέμε ότι **"το α είναι ισότιμο με το β ως προς modulo ν"** αν οι α, β είναι ισοϋπόλοιποι διαιρούμενοι με τον ν και θα γράφουμε :

$$\alpha \equiv \beta \, (mod \nu) \, .$$

Σε αντίθετη περίπτωση γράφουμε

$$\alpha \not\equiv \beta \, (mod \nu) \, .$$

Σχόλιο
Είναι προφανές από τον ορισμό ότι $\alpha \equiv \beta\,(mod\nu)$ αν και μόνο αν $\nu|\,(\alpha-\beta)$.

Ιδιότητες
Η σχέση της ισοτιμίας ικανοποιεί τις παρακάτω ιδιότητες για όλους τους ακεραίους $\alpha, \beta, \gamma, \nu$ με $\nu > 0$.

(i) $\alpha \equiv \alpha\,(mod\nu)$ (αναχλαστική ιδιότητα)
(ii) $\alpha \equiv \beta\,(mod\nu)$ αν και μόνο αν $\beta \equiv \alpha\,(mod\nu)$ (συμμετρική ιδιότητα)
(iii)Αν $\alpha \equiv \beta\,(mod\nu)$ και $\beta \equiv \gamma\,(mod\nu)$, τότε $\alpha \equiv \gamma\,(mod\nu)$ (μεταβατική ιδιότητα)
(iv) Αν $\alpha \equiv \beta\,(mod\nu)$ και $\gamma \equiv \delta\,(mod\nu)$, τότε $\alpha+\gamma \equiv \beta+\delta\,(mod\nu)$
(v) Αν $\alpha \equiv \beta\,(mod\nu)$ και $\gamma \equiv \delta\,(mod\nu)$, τότε $\alpha\gamma \equiv \beta\delta\,(mod\nu)$.
(vi) Αν $\alpha \equiv \beta\,(mod\nu)$ και $\delta \mid \nu$, $\delta > 0$, τότε $\alpha \equiv \beta\,(mod\delta)$
(vii) Αν $\alpha \equiv \beta\,(mod\nu)$, τότε $\alpha\gamma \equiv \beta\gamma\,(mod\nu\gamma)$, $\gamma > 0$.

Απόδειξη.
Οι αποδείξεις των ιδιοτήτων (i)–(v) είναι άμεση συνέπεια του ορισμού της ισοτιμίας.
Για τις ιδιότητες (vi) και (vii) έχουμε ότι αν $\alpha \equiv \beta(mod\nu)$, τότε $\nu \mid \alpha-\beta$, οπότε:
(vi) αν $\delta \mid \nu$, τότε $\delta \mid \alpha-\beta$ (ιδιότητα 1.2.1(ii)), οπότε $\alpha \equiv \beta\,(mod\delta)$.
(vii) $\nu\gamma \mid (\alpha-\beta)\,\gamma$ οπότε $\nu\gamma \mid (\alpha\gamma-\beta\gamma)$ ή $\alpha\gamma \equiv \beta\gamma\,(mod\nu\gamma)$.
Οι παραπάνω σχέσεις (i)–(iii) φανερώνουν ότι η ισοτιμία είναι μια **σχέση ισοδυναμίας** στο $\mathbf{Z}$, ενώ οι (iv)–(v) εκφράζουν ότι η ισοτιμία είναι συμβατή με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού. Οι τελευταίες ιδιότητες (vi)–(vii) αφορούν στη μεταβολή της κλάσης mod.

Άμεση εφαρμογή των ιδιοτήτων (iv)–(v) αποτελεί το ακόλουθο πόρισμα, που εκφράζει ότι τα πολυώνυμα αφήνουν αναλλοίωτη τη δομή των ισοτιμιών.

Πόρισμα 2.1.1
Αν f είναι πολυώνυμο με ακέραιους συντελεστές και $\alpha \equiv \beta\,(mod\nu)$ τότε $f\,(a) \equiv f\,(\beta)\,(mod\nu)$.

Τα ουδέτερα στοιχεία της πρόσθεσης και του πολλαπλασιασμού $(mod\nu)$ είναι το 0 και το 1 αντίστοιχα. Επίσης, έχουμε ότι $\alpha+(-\alpha)\equiv 0\,(mod\nu)$, δηλαδή ο $(-\alpha)$ είναι ο αντίθετος του α ως προς $(mod\nu)$.
Οι κλάσεις ισοδυναμίας που ορίσαμε στο Κεφάλαιο 1 μπορούν να γραφούν με το νέο συμβολισμό ως εξής:

$$\begin{aligned} Z_0 = &\quad \{x\in \mathbf{Z}/\ \ x\equiv 0(mod\nu)\}\\ Z_1 = &\quad \{x\in \mathbf{Z}/\ \ x\equiv 1(mod\nu)\}\\ &\quad \vdots\\ Z_{\nu-1} = &\quad \{x\in \mathbf{Z}/\ \ x\equiv (\nu-1)(mod\nu)\} \end{aligned}$$

δηλαδή κάθε ακέραιος x είναι ισότιμος με ένα και μοναδικό αριθμό από τους $0,1,2,\ldots(\nu-1)$ ως προς $(mod\nu)$.
Δύο ακέραιοι x,y θεωρούνται διαφορετικοί $(mod\nu)$ αν και μόνο αν $x\not\equiv y(mod\nu)$. Είναι δυνατόν να ορίσουμε τον αντίστροφο ενός ακεραίου ως προς $(mod\nu)$ ως εξής:

Ορισμός
Έστω $\alpha\in\mathbf{Z}$. Αν υπάρχει ακέραιος β, τέτοιος ώστε $\alpha\beta\equiv 1\,(mod\nu)$, τότε ο β λέγεται **αντίστροφος** του α ως προς $(mod\nu)$.

Είναι φανερό ότι δεν υπάρχει απαραίτητα ο αντίστροφος ενός ακεραίου ως προς $(mod\nu)$. Για παράδειγμα, οι 2 και 3 είναι αντίστροφοι $(mod5)$, αφού $2\cdot 3\equiv 1(mod5)$, ενώ η ισοτιμία $2\cdot\beta\equiv 1(mod10)$ δεν έχει λύση ως προς β, αφού για κάθε τιμή του β το 2β είναι άρτιος $(mod10)$, οπότε ο 2 δεν έχει αντίστροφο ως προς $(mod10)$.

Κατά συνέπεια ο νόμος της διαγραφής δεν ισχύει πάντοτε στις ισοτιμίες, δηλαδή δεν ισχύει η συνεπαγωγή:

$$Αν\ \alpha x\equiv \alpha y\,(mod\nu)\ \ τότε\ x\equiv y\,(mod\nu)\,.$$

Ισχύει όμως η παρακάτω ασθενέστερη μορφή του νόμου της διαγραφής.

Θεώρημα 2.1.2
(i) $\alpha x\equiv \alpha y(mod\nu)$ αν και μόνο αν $x\equiv y\left(mod\frac{\nu}{(\alpha,\nu)}\right)$.
(ii)Αν $\alpha x\equiv \alpha y(mod\nu)$ και $(\alpha,\nu)=1$, τότε $x\equiv y\,(mod\nu)$.
Απόδειξη.
(i) Αν $\alpha x\equiv \alpha y\,(mod\nu)$, τότε $\alpha x-\alpha y=\kappa\nu$, για κάποιον ακέραιο κ.

Επομένως έχουμε $\frac{\alpha}{(\alpha,\nu)}(x-y)=\frac{\nu}{(\alpha,\nu)}\kappa$, οπότε $\frac{\nu}{(\alpha,\nu)} \mid \frac{\alpha}{(\alpha,\nu)}(x-y)$.
Όμως $\left(\frac{\alpha}{(\alpha,\nu)},\frac{\nu}{(\alpha,\nu)}\right)=1$ (Πορ. 1.3.8), οπότε $\frac{\nu}{(\alpha,\nu)} \mid (x-y)$, από το Θεώρημα 1.3.9. Άρα $x\equiv y\left(mod\frac{\nu}{(\alpha,\nu)}\right)$.
Αντίστροφα, αν $x\equiv y\left(mod\frac{\nu}{(\alpha,\nu)}\right)$, τότε $\alpha x\equiv\alpha y\left(mod\frac{\alpha\nu}{(\alpha,\nu)}\right)$ (Ιδιότητα (vii)). Επειδή $\frac{\alpha}{(\alpha,\nu)}\in\mathbf{Z}$, θα είναι $\nu \mid \frac{\alpha\nu}{(\alpha,\nu)}$ και από την ιδιότητα (vi) έχουμε

$$\alpha x\equiv\alpha y\,(mod\nu)$$

(ii) Προκύπτει άμεσα από το (i).

Θεώρημα 2.1.3
Ο αντίστροφος του θετικού ακεραίου α ως προς $(mod\nu)$ υπάρχει αν και μόνο αν $(\alpha,\nu)=1$.
Απόδειξη.
Έστω ότι $(\alpha,\nu)=1$. Τότε θα υπάρχουν ακέραιοι κ, λ, ώστε να ισχύει $\kappa\alpha+\lambda\nu=1$ (Πορ. 1.3.5), οπότε $\kappa\alpha\equiv 1\,(mod\nu)$, δηλαδή ο κ είναι αντίστροφος του $\alpha(mod\nu)$.
Αντίστροφα, αν υπάρχει αριθμός β ώστε $\alpha\beta\equiv 1\,(mod\nu)$, τότε $\nu \mid (\alpha\beta-1)$.
Επειδή $(\alpha,\nu) \mid \nu$, θα έχουμε $(\alpha,\nu) \mid (\alpha\beta-1)$ (Θεωρ. 1.2.1(ii)).
Όμως $(\alpha,\nu) \mid \alpha$, οπότε $(\alpha,\nu) \mid \alpha\beta$, άρα και $(\alpha,\nu) \mid 1$, οπότε $(\alpha,\nu)=1$.

Παρατήρηση
Η παραπάνω απόδειξη αποτελεί και μέθοδο εύρεσης του αντιστρόφου.

Θεώρημα 2.1.4
Ο αντίστροφος ενός ακεραίου $\alpha>0$ ως προς $(mod\nu)$, αν υπάρχει, είναι μοναδικός $(mod\nu)$.
Απόδειξη.
Έστω ότι οι x,y είναι ταυτόχρονα αντίστροφοι του α ως προς $(mod\nu)$, δηλαδή $\alpha x\equiv 1\,(mod\nu)$ και $\alpha y\equiv 1\,(mod\nu)$.
Από την ιδιότητα (iv), έχουμε ότι $\alpha x-\alpha y\equiv 0\,(mod\nu)$ ή $\nu \mid \alpha(x-y)$, και επειδή $(\nu,\alpha)=1$ (προϋπόθεση ύπαρξης αντιστρόφου), προκύπτει ότι $\nu \mid (x-y)$ ή $x\equiv y\,(mod\nu)$ δηλαδή ο αντίστροφος είναι μοναδικός $(mod\nu)$.

Εφαρμογές 2.1

1. Να αποδείξετε ότι κάθε ακέραιος ικανοποιεί τουλάχιστον μία από τις παρακάτω ισοτιμίες :
   $x \equiv 0(mod2)$, $x \equiv 0(mod3)$, $x \equiv 1(mod4)$, $x \equiv 1(mod6)$, $x \equiv 11(mod12)$.

   Απόδειξη.

   Κάθε αριθμός γράφεται σε μία από τις μορφές

   $$x \equiv 0, 1, 2, \ldots, 11(mod12).$$

   Αν $x \equiv 0, 2, 4, 6, 8, 10(mod12)$ τότε $x \equiv 0(mod2)$.
   Αν $x \equiv 3, 9(mod12)$ τότε $x \equiv 0(mod3)$.
   Αν $x \equiv 1, 5(mod12)$ τότε $x \equiv 1(mod4)$.
   Αν $x \equiv 7(mod12)$ τότε $x \equiv 1(mod6)$.
   Έτσι παρατηρούμε ότι οι αρχικές ισοτιμίες καλύπτουν όλους τους ακεραίους.

2. Να βρείτε τους αντίστροφους modulo 19 των αριθμών
   (i) 3, (ii) 4, (iii) 7, (iv) 18.

   Λύση.

   Αναζητούμε έναν αριθμό x τέτοιο ώστε $3x \equiv 1(mod19)$.
   Από τον αλγόριθμο του Ευκλείδη για τον (3,19) βρίσκουμε ότι $1 \cdot 19 - 6 \cdot 3 = 1$ άρα $-6 \cdot 3 \equiv 1(mod19)$ συνεπώς ο αντίστροφος του 3 είναι ο $-6(mod19)$ ή ο $13(mod19)$.
   Όμοια βρίσκουμε τους αντίστροφους των 4,7,18 οι οποίοι είναι οι 5,11,18 $(mod19)$ αντίστοιχα.

3. Έστω ένας φυσικός κ και ένας περιττός πρώτος p. Να αποδειχθεί ότι οι λύσεις της $x^2 \equiv 1(modp^\kappa)$ είναι $x \equiv \pm 1(modp^\kappa)$.

   Απόδειξη.

   Η ισοτιμία $x^2 \equiv 1(modp^\kappa)$ γράφεται $(x-1)(x+1) \equiv 0(modp^\kappa)$.
   Όμως ο p δεν μπορεί να διαιρεί ταυτόχρονα τους $(x-1)$ και $(x+1)$ αφού τότε θα διαιρούσε και τη διαφορά τους, δηλαδή το 2, αδύνατο

αφού $p \geq 3$. Έτσι έχουμε ότι:

$$\begin{array}{llll} \text{είτε} & p^x \mid (x-1), & \text{οπότε} & x \equiv 1(mod p^x) \\ \text{είτε} & p^x \mid (x+1), & \text{οπότε} & x \equiv -1(mod p^x). \end{array}$$

4. Αν $\nu \equiv 3(mod 4)$, να αποδειχθεί ότι ο φυσικός ν είναι αδύνατο να γραφεί ως άθροισμα των τετραγώνων δύο ακεραίων.

Απόδειξη.

Έστω $\nu = x^2 + y^2$. Γνωρίζουμε ότι οι x^2, y^2 θα είναι ισότιμοι με 0 ή 1 $(mod 4)$ ανάλογα με το αν οι x, y είναι άρτιοι ή περιττοί. Έτσι, ο $x^2 + y^2$ δε μπορεί να είναι ισότιμος με 3 $(mod 4)$.

5. Να αποδειχθεί ότι για κάθε φυσικό ν ο αριθμός $5^{2\nu+1} + 11^{2\nu+1} + 17^{2\nu+1}$ είναι πολλαπλάσιο του 33.

Απόδειξη.

Έχουμε (ιδιότητα (iv)):

$$\begin{aligned} 5^{2\nu+1} + 11^{2\nu+1} + 17^{2\nu+1} &\equiv 2^{2\nu+1} + 2^{2\nu+1} + 2^{2\nu+1}(mod 3) \\ &\equiv 3 \cdot 2^{2\nu+1}(mod 3) \\ &\equiv 0(mod 3) \end{aligned}$$

και

$$\begin{aligned} 5^{2\nu+1} + 11^{2\nu+1} + 17^{2\nu+1} &\equiv (11-6)^{2\nu+1} + 11^{2\nu+1} + \\ &\quad + (11+6)^{2\nu+1}(mod 11) \\ &\equiv (-6)^{2\nu+1} + 6^{2\nu+1}(mod 11) \\ &\equiv 0(mod 11) \end{aligned}$$

Εφόσον οι 3, 11 είναι σχετικά πρώτοι, καταλήγουμε ότι $33 \mid (5^{2\nu+1} + 11^{2\nu+1} + 17^{2\nu+1})$.

6. Να αποδειχθεί ότι για κάθε φυσικό ν ο αριθμός $N = 2^{2\nu} + 24\nu - 10$ είναι πολλαπλάσιο του 18.

Απόδειξη.

Αρχικά παρατηρούμε ότι ο N είναι άρτιος. Επιπλέον στο διώνυμο $(3-1)^{2\nu} = 3^{2\nu} - 2\nu \cdot 3^{2\nu-1} + \ldots - 2\nu \cdot 3 + 1$ όλοι οι όροι του εκτός

των δύο τελευταίων, περιέχουν δυνάμεις του 3 μεγαλύτερες ή ίσες του 3^2.
Επομένως,

$$\begin{aligned} 2^{2\nu} + 24\nu - 10 &\equiv (3-1)^{2\nu} + (18\nu - 9) + 6\nu - 1 \\ &\equiv (-2\nu \cdot 3 + 1)(mod 9) + (6\nu - 1)(mod 9) \\ &\equiv (-6\nu + 1 + 6\nu - 1)(mod 9) \\ &\equiv 0 \ (mod 9). \end{aligned}$$

Άρα $9 \mid N$, οπότε και $18 \mid N$, αφού N άρτιος.

7. Αν α είναι ένας φυσικός αριθμός με $(\alpha, 6) = 1$, να αποδειχθεί ότι $\alpha^2 \equiv 1(mod 6)$.

Απόδειξη.

Αφού ο φυσικός α είναι σχετικά πρώτος με τον αριθμό 6, θα είναι προφανώς περιττός και όχι πολλαπλάσιος του 3.
Άρα $\alpha \equiv \pm 1(mod 6)$, οπότε $\alpha^2 \equiv 1(mod 6)$.

8. Να βρείτε τα τρία τελευταία ψηφία του αριθμού 2^{12102}.

Λύση.

Θα προσπαθήσουμε να βρούμε έναν τριψήφιο αριθμό, έτσι ώστε η διαφορά του από το 2^{12102} να είναι πολλαπλάσιο του 1000. Έχουμε $2^{12102} = 2^2(2^{10})^{1210} = 4(1024)^{1210}$.
Όμως

$$\begin{aligned} 24^{11} &= 24(576)^5 \\ &= 24(576)(576^2)^2 \\ &\equiv 24(576)(776)^2 \quad (mod 1000) \\ &\equiv 24(576)(176) \quad (mod 1000) \\ &\equiv 24 \quad (mod 1000) \end{aligned}$$

Έτσι

$$\begin{aligned} 2^{12102} &\equiv 4(24)^{1210} \quad (mod 1000) \\ &\equiv 4(24^{11})^{110} \quad (mod 1000) \\ &\equiv 4(24)^{110} \quad (mod 1000) \\ &\equiv 4(24^{11})^{10} \quad (mod 1000) \\ &\equiv 4(24)^{10} \quad (mod 1000) \\ &\equiv 4(576)(176) \quad (mod 1000) \\ &\equiv 504 \quad (mod 1000) \end{aligned}$$

όπου $24^{10} \equiv (576)(176)(mod 1000)$ από τον υπολογισμό του 24^{11}. Έτσι τα τελευταία 3 ψηφία του 2^{12102} είναι 504.

9. Να αποδειχθεί ότι ο αριθμός $2222^{5555} + 5555^{2222}$ είναι πολλαπλάσιο του 7.

Απόδειξη.

Παρατηρούμε ότι $2222 \equiv 3(mod 7)$ και $5555 \equiv 4(mod 7)$. Επιπλέον ισχύει ότι

$$3^6 \equiv 729 \equiv 1(mod 7) \quad \text{και}$$
$$4^3 \equiv 64 \equiv 1(mod 7).$$

Άρα

$$\begin{aligned} 2222^{5555} + 5555^{2222} &\equiv 3^{5555} + 4^{2222}(mod 7) \\ &\equiv 3^5 \cdot (3^6)^{925} + 4^2 \cdot (4^3)^{740}(mod 7) \\ &\equiv 3^5 + 4^2(mod 7) \\ &\equiv 243 + 16(mod 7) \\ &\equiv 259(mod 7) \\ &\equiv 0(mod 7). \end{aligned}$$

Επομένως, ο αριθμός $2222^{5555} + 5555^{2222}$ είναι πολλαπλάσιο του 7.

Παρατήρηση

Η άσκηση αυτή έχει δοθεί και στις Γενικές του 1ου Κεφαλαίου, όπου η λύση της είναι δυσκολότερη και στερείται μεθόδου.

Ασκήσεις 2.1

Α' Ομάδα

1. Έστω ένας φυσικός κ και ένας πρώτος p. Να αποδειχθεί ότι οι μόνες λύσεις της $x^2 \equiv x(mod p^\kappa)$ είναι οι $x \equiv 0$ ή $1(mod p^\kappa)$.

2. Να αποδειχθεί ότι για κάθε φυσικό ν το τελευταίο ψηφίο του ν^2 είναι ένα από τα ψηφία 0, 1, 4, 5, 6, 9.

3. Με χρήση των ισοτιμιών να αποδειχθούν τα παρακάτω:

   (i) $13 \mid (145^6 + 1)$ (ii)$431 \mid (2^{43} - 1)$
   (iii)$233 \mid (2^{29} - 1)$ (iv)$167 \mid (2^{83} - 1)$.

4. Αν ο φυσικός ν είναι σχετικά πρώτος με τον αριθμό 7, τότε να αποδειχθεί ότι $7 \mid (\nu^6 - 1)$ και $7 \mid (\nu^{12} - 1)$.

5. Αν ν και μ είναι δύο φυσικοί αριθμοί και p ένας πρώτος, τότε ισχύει:
   $$(\nu + \mu)^p \equiv \nu^p + \mu^p (mod p).$$

6. Βρείτε τα τρία τελευταία ψηφία του αριθμού 2^{10000}.

7. Να υπολογισθεί το υπόλοιπο της διαίρεσης του $N = 9^{1998} + 17^{1999}$ διά του 8.

8. Να αποδείξετε ότι για κάθε σύνθετο φυσικό $\nu > 4$ ισχύει ότι
   $$(\nu - 1)! \equiv 0(mod \nu).$$

9. Αν $\alpha \equiv \beta(mod \nu)$, να αποδειχθεί ότι $(\alpha, \nu) = (\beta, \nu)$.

10. Αν ν, μ είναι δύο φυσικοί αριθμοί, να αποδειχθεί ότι:
    $$\mu^{2\nu} \equiv 1(mod(\mu + 1)).$$

Β' Ομάδα

11. Να αποδειχθεί ότι για κάθε φυσικό $\nu > 0$ ισχύει

$$7 \mid (5^{2\nu} + 3 \cdot 2^{5\nu-2})$$

12. Να εξετάσετε ποιες από τις παρακάτω ισοτιμίες ισχύουν:

(i) $91 \equiv 1(mod 3)$

(ii) $75 \equiv 68(mod 7)$

(iii) $671 \equiv 1(mod 37)$

(iv) $-28 \equiv 2(mod 3)$

(v) $1 \equiv 71(mod 2)$

(vi) $-40 \equiv 26(mod 11)$

(vii) $-20 \equiv -60(mod 80)$

(viii) $11 \equiv 111(mod 11)$

13. Αν p ένας περιττός πρώτος, να αποδείξετε ότι ο x έχει αντίστροφο modulo p τον εαυτό του αν και μόνο αν $x \equiv 1$ ή $-1(mod p)$.

14. α) Να αποδείξετε ότι αν οι αριθμοί p και $8p - 1$ είναι πρώτος, τότε ο $8p + 1$ είναι σύνθετος.

β) Να αποδείξετε ότι αν οι αριθμοί p και $8p^2 + 1$ είναι πρώτοι, τότε ο $8p^2 - 1$ είναι πρώτος.

15. Να αποδείξετε ότι αν οι συντελεστές της εξίσωσης $\alpha x^2 + \beta x + \gamma = 0$ είναι περιττοί ακέραιοι τότε η εξίσωση δεν έχει ρητές λύσεις.

16. (α) Να βρείτε όλους τους φυσικούς ν για τους οποίους ο $2^\nu - 1$ διαιρείται με το 7.

(β) Να αποδείξετε ότι δεν υπάρχει φυσικός ν για τον οποίο ο $2^\nu + 1$ να διαιρείται με το 7. (6η ΔΜΟ, 1964, Μόσχα)

17. Να βρεθούν οι λύσεις της εξίσωσης $x_1^4 + x_2^4 + \ldots + x_{14}^4 = 15999$, όπου $x_1,\ x_2,\ \ldots, x_{14}$ φυσικοί.

18. Να βρείτε μία μη σταθερή αριθμητική πρόοδο θετικών ακεραίων, απείρου μήκους, τέτοια ώστε κάθε όρος της να μην γράφεται ως άθροισμα δύο τετραγώνων ή δύο κύβων θετικών ακεραίων.

19. Να βρείτε τι ώρα είναι

    (i) 100 ώρες μετά τα μεσάνυχτα

    (ii) 1000 ώρες μετά τις 3 το μεσημέρι

    (iii) 1000 ώρες πριν τις 5 το πρωί.

20. Να αποδείξετε ότι για κάθε φυσικό ν ισχύει ότι: $4^{\nu} \equiv 1 + 3\nu (mod 9)$.

2.2 Η γραμμική ισοτιμία $\alpha x \equiv \beta\,(mod\nu)$

Το αμέσως επόμενο βήμα μετά τον ορισμό και τις αλγεβρικές ιδιότητες της ισοτιμίας, είναι η επίλυση "εξισώσεων".
Ας θεωρήσουμε τη γραμμική ισοτιμία

$$\alpha x \equiv \beta\,(mod\nu)$$

όπου α, β ακέραιοι, ν φυσικός, $\nu > 0$ και x άγνωστος ακέραιος.
Θα λέμε ότι ο ακέραιος x_0 είναι **λύση** της εξίσωσης $\alpha x \equiv \beta(mod\nu)$, αν ισχύει ότι $\alpha x_0 \equiv \beta(mod\nu)$.
Κατ' αρχήν παρατηρούμε ότι αν x_0 είναι μια λύση της ισοτιμίας, τότε κάθε ακέραιος που ικανοποιεί τη σχέση

$$x = x_0 + \kappa\nu, \kappa \in \mathbf{Z}$$

αποτελεί επίσης λύση, αφού επαληθεύει την αρχική ισοτιμία.
Αν λοιπόν η αρχική ισοτιμία έχει λύση, τότε έχει άπειρες λύσεις, αφού κάθε ακέραιος της μορφής $x = x_0 + \kappa\nu,\ \kappa \in \mathbf{Z}$, είναι λύση, δηλαδή το σύνολο των λύσεων είναι μία κλάση ισοδυναμίας $mod\nu$. Έτσι γράφουμε τη λύση στη μορφή $x_0(mod\nu)$.
Στην προσπάθειά μας να λύσουμε τη γραμμική ισοτιμία διακρίνουμε τις περιπτώσεις:

- $\alpha \equiv 0(mod\nu)$.
  Τότε για κάθε ακέραιο x έχουμε $\alpha x \equiv 0\,(mod\nu)$, οπότε αναγκαία προϋπόθεση για να υπάρχει λύση είναι $\beta \equiv 0(mod\nu)$.
  Διακρίνουμε τις υποπεριπτώσεις :
  1. $\beta \equiv 0(mod\nu)$
  Στην περίπτωση αυτή η ισοτιμία έχει λύση όλους τους ακέραιους, δηλαδή υπάρχουν ν διαφορετικές λύσεις, οι

  $$0, 1, 2, \ldots, (\nu - 1)\,(mod\nu)$$

  2. $\beta \not\equiv 0(mod\nu)$
  Στην περίπτωση αυτή η ισοτιμία είναι αδύνατη.

- $\alpha \not\equiv 0\,(mod\nu)$.
  Τότε διακρίνουμε τις υποπεριπτώσεις :

1. $(\alpha,\nu)=1$
   Από το Θεώρημα 2.1.3 υπάρχει μοναδικός αντίστροφος γ του α, τέτοιος ώστε $\alpha\gamma \equiv 1\,(mod\nu)$.
   Έτσι έχουμε :

$$\begin{aligned} \alpha x &\equiv \beta\,(mod\nu) \quad \text{ή} \\ \alpha\gamma x &\equiv \beta\gamma\,(mod\nu) \quad \text{ή} \\ 1x &\equiv \beta\gamma\,(mod\nu)\,, \end{aligned}$$

   συνεπώς η ισοτιμία έχει λύση την $x_0 \equiv \beta\gamma\,(mod\nu)$.
   Έστω ότι η ισοτιμία έχει μια δεύτερη λύση τότε $\alpha x_0 - \alpha y_0 \equiv 0(mod\nu)$, άρα $\nu \mid \alpha(x_0 - y_0)$ και επειδή $(\alpha,\nu)=1$ θα είναι $\nu \mid (x_0 - y_0)$, άρα $x_0 \equiv y_0(mod\nu)$.
   Η λύση x_0 της ισοτιμίας είναι συνεπώς μοναδική ως προς $(mod\nu)$.

2. $(\alpha,\nu)=\delta>1$
   Τότε $\alpha x \equiv \beta\,(mod\nu)$, δηλαδή $\nu \mid (\alpha x - \beta)$ και επειδή $\delta \mid \nu$, $\delta \mid \alpha$ αναγκαία συνθήκη για να υπάρχει λύση είναι $\delta \mid \beta$.

   Στην περίπτωση αυτή η ισοτιμία γράφεται ισοδύναμα

$$\frac{\alpha}{\delta}x \equiv \frac{\beta}{\delta}\left(mod\frac{\nu}{\delta}\right),$$

   όπου $\left(\frac{\alpha}{\delta},\frac{\nu}{\delta}\right)=1$. Από την προηγούμενη υποπερίπτωση, η εξίσωση αυτή έχει μοναδική λύση $x_0\left(mod\frac{\nu}{\delta}\right)$. Άρα οι λύσεις της αρχικής ισοτιμίας είναι οι αριθμοί $x = x_0(mod\frac{\nu}{\delta})$. Αυτή η σχέση δίνει δ διαφορετικές λύσεις $(mod\nu)$, οι οποίες είναι οι εξής :

$$\begin{gathered} x_0\,(mod\nu) \\ x_0 + \frac{\nu}{\delta}\,(mod\nu) \\ x_0 + \frac{2\nu}{\delta}\,(mod\nu) \\ \vdots \\ x_0 + \frac{(\delta-1)\,\nu}{\delta}\,(mod\nu) \end{gathered}$$

Στην περίπτωση που ο δ δεν διαιρεί τον β η ισοτιμία είναι αδύνατη.

Παρατηρήσεις
1) Αν η ισοτιμία $ax \equiv \beta(mod\nu)$ είναι επιλύσιμη και $\alpha \not\equiv 0(mod\nu)$ τότε έχει ακριβώς (α, ν) διαφορετικές λύσεις.
2) Η επίλυση της γραμμικής ισοτιμίας $ax \equiv \beta(mod\nu)$ παρουσιάζει ομοιότητες με τη λύση της εξίσωσης $ax = \beta$ στους πραγματικούς. Αυτή η εξίσωση έχει λύση μόνο αν ο α έχει αντίστροφο δηλαδή $\alpha \neq 0$ (εκτός από την τετριμμένη περίπτωση $\alpha = \beta = 0$) και η λύση της είναι μοναδική αφού ο αντίστροφος είναι μοναδικός. Η γραμμική ισοτιμία έχει λύση αν ο α έχει αντίστροφο (mod ν) ή εάν η ισοτιμία μπορεί να μετασχηματισθεί σε μία άλλη ισοτιμία που να ικανοποιεί αυτή την προϋπόθεση.

Σύστημα γραμμικών ισοτιμιών

Η επίλυση ενός συστήματος γραμμικών ισοτιμιών βασίζεται στην ενοποίηση των διαφορετικών κλάσεων ισοϋπολοίπων.

Θεώρημα 2.2.1 (Κινέζικο θεώρημα υπολοίπων)
Έστω $\nu_1, \nu_2, \ldots, \nu_\varkappa$ θετικοί ακέραιοι ανά δύο σχετικά πρώτοι μεταξύ τους, και $\alpha_1, \alpha_2, \ldots, \alpha_\varkappa$ ακέραιοι. Το σύστημα γραμμικών ισοτιμιών:

$$x \equiv \alpha_1 \,(mod\nu_1)$$

$$x \equiv \alpha_2 \,(mod\nu_2)$$

$$\vdots$$

$$x \equiv \alpha_\varkappa \,(mod\nu_\varkappa)$$

έχει μοναδική λύση $(mod\,(\nu_1 \nu_2 \cdots \nu_\varkappa))$

Απόδειξη.

Έστω $\nu = \nu_1 \cdot \nu_2 \cdot \ldots \cdot \nu_\varkappa$. Για κάθε $i = 1, 2, \ldots, \varkappa$ έχουμε $\left(\frac{\nu}{\nu_i}, \nu_i\right) = 1$, οπότε υπάρχει β_i ώστε $\frac{\nu}{\nu_i}\beta_i \equiv 1\,(mod\nu_i)$, δηλαδή ο $\frac{\nu}{\nu_i}$ αντιστρέφεται ως προς $(mod\nu_i)$.

Επίσης $\frac{\nu}{\nu_i}\beta_i \equiv 0\,(mod\nu_i)$ για κάθε $i \neq j$.

Ο αριθμός $x_0 = \frac{\nu}{\nu_1}\beta_1\alpha_1 + \frac{\nu}{\nu_2}\beta_2\alpha_2 + \ldots + \frac{\nu}{\nu_\varkappa}\beta_\varkappa\alpha_\varkappa$ είναι λύση, αφού για κάθε

$i = 1, 2, ..., \varkappa$ έχουμε ότι:

$$\begin{aligned} x_0 &\equiv \tfrac{\nu}{\nu_1}\beta_1\alpha_1 + \tfrac{\nu}{\nu_2}\beta_2\alpha_2 + \ldots + \tfrac{\nu}{\nu_\varkappa}\beta_\varkappa\alpha_\varkappa \pmod{\nu_i} \\ &\equiv \tfrac{\nu}{\nu_i}\beta_i\alpha_i \,(mod\nu_i) \\ &\equiv \alpha_i \,(mod\nu_i) \end{aligned}$$

Αν τώρα x_0, x_1 είναι δύο διαφορετικές λύσεις του συστήματος ισοτιμιών, τότε $x_0 \equiv x_1 \,(mod\nu_i)$ οπότε $\nu_i \mid (x_0 - x_1)$ για κάθε $i = 1, 2, \ldots, \varkappa$. Αφού οι $\nu_1, \nu_2, \ldots, \nu_\varkappa$ είναι σχετικά πρώτοι ανά δύο, προκύπτει ότι $\nu \mid (x_0 - x_1)$, δηλαδή $x_0 \equiv x_1 (mod\nu)$. Συνεπώς η λύση είναι μοναδική ως προς $(mod\nu)$.

Εφαρμογές 2.2

1. Να λυθούν οι παρακάτω γραμμικές ισοτιμίες:
   (i) $6x \equiv 2\,(mod 7)$
   (ii) $6x \equiv 3\,(mod 9)$
   (iii) $6x \equiv 2\,(mod 9)$

   Λύση.

   (i) Επειδή (6,7)=1 υπάρχει μοναδική λύση. Από τον αλγόριθμο του Ευκλείδη (ή με παρατήρηση) έχουμε ότι $1 = 1 \cdot 7 + (-1)\,6$, οπότε $(-1)\,6 \equiv 1\,(mod 7)$. Δηλαδή το $-1 \equiv 6\,(mod 7)$ είναι ο αντίστροφος του 6 (mod7).
   Έτσι έχουμε

   $$6 \cdot 6x \equiv 6 \cdot 2\,(mod 7) \text{ ή } x \equiv 12\,(mod 7) \text{ ή } x \equiv 5\,(mod 7)\,.$$

   (ii) Επειδή (6,9)=3 και $3 \mid 3$ υπάρχουν ακριβώς τρεις λύσεις.
   Από τον αλγόριθμο του Ευκλείδη έχουμε ότι $3 = (-1) \cdot 6 + 1 \cdot 9$ ή $1 = (-1) \cdot 2 + 1 \cdot 3$ άρα $(-1) \cdot 2 \equiv 1\,(mod 3)$.
   Έτσι $6x \equiv 3\,(mod 9)$ ή $2x \equiv 1\,(mod 3)$ ή $2 \cdot 2x \equiv 2\,(mod 3)$ ή $x \equiv 2\,(mod 3)$. Άρα οι λύσεις $(mod 9)$ είναι: $x = 2$, $x = 5$, $x = 8$.
   (iii) Επειδή $(6, 9) = 3$ και $3 \not| 2$ η ισοτιμία είναι αδύνατη.

2. Να λυθεί το σύστημα γραμμικών ισοτιμιών:

   $$\left\{ \begin{array}{lll} x & \equiv 2 & (mod 9) \\ x & \equiv 1 & (mod 5) \\ x & \equiv 2 & (mod 4) \end{array} \right\}$$

   Λύση.

   Έχουμε $\nu = 9 \cdot 5 \cdot 4 = 180$. Υπολογίζουμε τους αντίστροφους (π.χ. χρησιμοποιώντας τον αλγόριθμο του Ευκλείδη ή με δοκιμές) των αριθμών $180/9 = 20$, $180/5 = 36$, $180/4 = 45$, modulo $9, 5, 4$ αντίστοιχα, οι οποίοι είναι οι 5, 1, 1 αντίστοιχα. Ο αριθμός λοιπόν $20 \cdot 5 \cdot 2 + 36 \cdot 1 \cdot 1 + 45 \cdot 1 \cdot 2 (mod 180)$ ή $146 (mod 180)$ είναι η μοναδική λύση του συστήματος.

3. Να λύσετε το παρακάτω σύστημα :

$$\left\{ \begin{array}{lll} x & \equiv 1 & (mod 3) \\ 3x & \equiv 1 & (mod 4) \\ 4x & \equiv 2 & (mod 5) \end{array} \right\}$$

Λύση.

Λύνοντας καθεμία από τις ισοτιμίες ξεχωριστά παίρνουμε το σύστημα

$$\begin{array}{lll} x & \equiv 1 & (mod 3) \\ x & \equiv 3 & (mod 4) \\ x & \equiv 3 & (mod 5) \end{array}$$

το οποίο έχει μοναδική λύση $(mod 60)$.
Οι αντίστροφοι των αριθμών $20(mod 3)$, $15(mod 4)$ και $12(mod 5)$ είναι οι 2, 3, 3 αντίστοιχα.
Άρα η μοναδική λύση του συστήματος είναι η
$20 \cdot 2 \cdot 1 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 3 (mod 60) \equiv 43 (mod 60)$.

Ασκήσεις 2.2

Α' Ομάδα

1. Να λυθούν οι παρακάτω γραμμικές ισοτιμίες :
   (i) $15x \equiv 24\,(mod 35)$
   (ii) $20x \equiv 30\,(mod 4)$
   (iii) $353x \equiv 254\,(mod 400)$

2. Να λυθούν τα συστήματα ισοτιμιών:

$$\text{(i)}\left\{\begin{array}{lll} x & \equiv 1 & (mod 5) \\ x & \equiv 3 & (mod 7) \\ x & \equiv 5 & (mod 2) \end{array}\right\}, \text{(ii)}\left\{\begin{array}{lll} 2x & \equiv 6 & (mod 7) \\ 2x & \equiv 1 & (mod 3) \\ 5x & \equiv 4 & (mod 19) \end{array}\right\}$$

3. Να λυθούν τα συστήματα ισοτιμιών:

$$\text{(i)}\left\{\begin{array}{lll} x & \equiv 2 & (mod 3) \\ x & \equiv 3 & (mod 5) \\ x & \equiv 5 & (mod 2) \end{array}\right\}, \text{(ii)}\left\{\begin{array}{lll} x & \equiv 1 & (mod 4) \\ x & \equiv 0 & (mod 3) \\ x & \equiv 5 & (mod 7) \end{array}\right\}$$

$$\text{(iii)}\left\{\begin{array}{lll} x & \equiv 3 & (mod 4) \\ x & \equiv 5 & (mod 7) \\ x & \equiv 2 & (mod 9) \end{array}\right\}, \text{(iv)}\left\{\begin{array}{lll} x & \equiv 1 & (mod 9) \\ x & \equiv 2 & (mod 10) \\ x & \equiv 3 & (mod 11) \end{array}\right\}$$

4. Να βρείτε όλους τους ακέραιους οι οποίοι αφήνουν υπόλοιπο 1 διαιρούμενοι με το 2, υπόλοιπο 2 διαιρούμενοι με το 3 και υπόλοιπο 3 διαιρούμενοι με το 5.

Β' Ομάδα

5. **(Γενίκευση Κινέζικου Θεωρήματος)**
   Να αποδείξετε ότι οι γραμμικές ισοτιμίες $x \equiv \alpha_i\,(mod\nu_i)$, με $i = 1, 2, \ldots, \kappa$ έχουν κοινή λύση αν και μόνο αν $(\nu_i, \nu_j) \mid (\alpha_i - \alpha_j)$ για κάθε $i \neq j$. Στην περίπτωση που υπάρχει λύση, αυτή είναι μοναδική $(mod\,[\nu_1, \nu_2, \ldots, \nu_\kappa])$.

6. Έστω $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ η κανονική μορφή του φυσικού ν. Να αποδειχθεί ότι κάθε κοινή λύση του συστήματος των γραμμικών ισοτιμιών $x \equiv \alpha(mod p_j^{\alpha_j})$, για j=1,2,...,κ είναι λύση της $x \equiv \alpha(mod\nu)$.

7. Να εξετάσετε αν μπορούμε να βρούμε 21 διαδοχικούς φυσικούς καθένας από τους οποίους να έχει έναν ή περισσότερους πρώτους παράγοντες p, με $2 \leq p \leq 13$.

2.3 Η συνάρτηση φ του Euler

Στο Κεφάλαιο 1 διαμερίσαμε τους ακέραιους σε κλάσεις ανάλογα με το υπόλοιπο που αφήνουν διαιρούμενοι με τον αριθμό ν, οπότε σχηματίσαμε τα ν σύνολα (κλάσεις ισοδυναμίας):

$$Z_0 = \{x/x \equiv 0\,(mod\nu)\}$$

$$Z_1 = \{x/x \equiv 1\,(mod\nu)\}$$

$$\vdots$$

$$Z_{\nu-1} = \{x/x \equiv \nu - 1\,(mod\nu)\}\,.$$

Στην προηγούμενη παράγραφο ωστόσο παρατηρήσαμε ότι ως προς τον πολλαπλασιασμό δεν υπάρχει πάντοτε ο αντίστροφος. Ικανή και αναγκαία συνθήκη για να αντιστρέφεται ο ακέραιος $\alpha \neq 0$ ως προς *modulo* ν είναι (α,ν)=1. Αν λοιπόν από τα παραπάνω σύνολα κρατήσουμε μόνο τα παρακάτω:

$$\{x/x \equiv r_i\,(mod\nu)\}\,,\ \mu\varepsilon\ \ (r_i, \nu) = 1$$

τότε στα σύνολα αυτά ισχύουν όλοι οι συνηθισμένοι κανόνες της άλγεβρας ως προς την πράξη του πολλαπλασιασμού (δηλαδή ύπαρξη αντιστρόφου και κανόνας διαγραφής). Το σύνολο $\{r_i\}$ ονομάζεται συνήθως "ανηγμένο σύστημα υπολοίπων $(mod\nu)$".

Ορισμός

Το πλήθος των παραπάνω συνόλων ορίζεται ως $\varphi(\nu)$ και εξαρτάται μόνο από το ν.

Με άλλα λόγια, $\varphi(\nu)$ είναι το πλήθος των αριθμών του συνόλου $\{1, 2, \ldots, \nu - 1\}$ που είναι σχετικά πρώτοι με το ν.

Η συνάρτηση $\varphi : N \longrightarrow N$ ονομάζεται **συνάρτηση φ του Euler**. Στην περίπτωση που $\nu = 1$ ορίζουμε $\varphi(1) = 1$.

Για παράδειγμα έχουμε $\varphi(12) = 4$, αφού ο αριθμός 12 είναι σχετικά πρώτος με τους 1, 5, 7, 11, ενώ δεν είναι με τους 2, 3, 4, 6, 8, 9, 10.

Επίσης για κάθε πρώτο p ισχύει $\varphi(p) = p - 1$ αφού ο p είναι σχετικά πρώτος με τους $1, 2, 3, \ldots, p - 1$.

Θεώρημα 2.3.1
Ο αριθμός $\varphi(\nu)$ για $\nu \geq 3$ είναι άρτιος.

Απόδειξη.

Έστω $r_1, r_2, \ldots, r_{\varphi(\nu)}$ οι αριθμοί του συνόλου $\{1, 2, \ldots, \nu\}$ που είναι σχετικά πρώτοι με το ν.
Για κάθε αριθμό r_i θα υπάρχει μοναδικός αντίστροφος του *modulo* ν, δηλαδή ένας αριθμός α τέτοιος ώστε $r_i\alpha \equiv 1\,(mod\nu)$ (Θεώρημα 2.1.3).
Άρα και ο α θα είναι κάποιος από τους $\{r_\varkappa\}$, αφού ο α αντιστρέφεται (έχει αντίστροφο τον r_i θα ισχύει (α,ν)=1, οπότε θα ανήκει στο σύνολο $\{r_\varkappa\}$).
Ας βρούμε ποιοι αριθμοί έχουν ως αντίστροφο τον εαυτό τους. Έστω $x^2 \equiv 1\,(mod\nu)$. Τότε $\nu \mid (x^2-1)$ ή $\nu \mid (x-1)(x+1)$. Αν p_i είναι ένας πρώτος παράγοντας του ν, τότε $p_i \mid x-1$ ή $p_i \mid x+1$, άρα $x \equiv \pm 1\,(mod p_i)$.
Έτσι από το Θεώρημα 2.2.1 θα είναι $x \equiv \pm 1\,(mod p_1 p_2 \ldots)$ δηλαδή $x \equiv \pm 1\,(mod\nu)$. Αυτό σημαίνει ότι μόνο οι αριθμοί 1 και -1 (δηλαδή $\nu - 1$) μπορούν να έχουν για αντίστροφο τον εαυτό τους.
Πράγματι, $1^2 \equiv (\nu-1)^2 \equiv 1\,(mod\nu)$. Έτσι λοιπόν το σύνολο $\{r_\varkappa\}$ αποτελείται από το 1, το $\nu - 1$ και ζεύγη αντίστροφων ακεραίων, δηλαδή έχει άρτιο πλήθος στοιχείων.

Μελετώντας την τιμή της συνάρτησης Euler σε δυνάμεις πρώτων μπορούμε να αποδείξουμε ότι είναι πολλαπλασιαστική συνάρτηση και να βρούμε την ευκολότερη μέθοδο προσδιορισμού της για τυχαίο φυσικό αριθμό.

Θεώρημα 2.3.2
Αν ο p είναι πρώτος και ο α είναι ένας τυχαίος φυσικός, τότε έχουμε: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right)$.

Απόδειξη.

Αν ο αριθμός p είναι πρώτος, τότε από τους $1, 2, 3, \ldots, p^\alpha - 1$ μόνο οι αριθμοί $p, 2p, \ldots, (p^{\alpha-1}-1)p$ δεν είναι σχετικά πρώτοι με τον p^α. Άρα

$$\varphi(p^\alpha) = p^\alpha - 1 - (p^{\alpha-1}-1) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right).$$

Θεώρημα 2.3.3
Αν α, β θετικοί ακέραιοι με $(\alpha, \beta) = 1$, τότε $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$.
Απόδειξη.
Έστω $\varkappa = \varphi(\alpha)$, $\lambda = \varphi(\beta)$ και $r_1, r_2, \ldots, r_\varkappa$, $s_1, s_2, \ldots, s_\lambda$ οι αριθμοί των συνόλων $\{1, 2, \ldots, \alpha\}, \{1, 2, \ldots, \beta\}$ που είναι σχετικά πρώτοι με τους α, β αντίστοιχα. Αν ο x είναι σχετικά πρώτος με τον $\alpha\beta$, τότε προφανώς $(x, \alpha) = (x, \beta) = 1$, οπότε $x \equiv r_i \,(mod\alpha)$ και $x \equiv s_j \,(mod\beta)$ για $i = 1, 2, \ldots, \varkappa$ και $j = 1, 2, \ldots, \lambda$.
Αντίστροφα, αν $x \equiv r_i \,(mod\alpha)$ και $x \equiv s_j \,(mod\beta)$, τότε $(x, \alpha\beta) = 1$. Άρα όλοι οι αριθμοί x που είναι σχετικά πρώτοι με τον αβ προσδιορίζονται αν λύσουμε το σύστημα $x \equiv r_i \,(mod\alpha)$ και $x \equiv s_j \,(mod\beta)$ για κάθε τιμή των i, j. Όμως από το Θεώρημα 2.2.1, κάθε επιλογή των i, j δίνει διαφορετικές τιμές $mod(\alpha\beta)$, οπότε παίρνουμε $\varkappa\lambda$ διαφορετικούς αριθμούς, δηλαδή $\varphi(\alpha\beta) = \varkappa\lambda$.

Πόρισμα 2.3.4
Αν $\nu \geq 2$, τότε $\varphi(\nu) = \nu\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_\varkappa}\right)$, όπου $p_1, \ldots, p_\varkappa$ όλοι οι πρώτοι που διαιρούν τον ν.
Απόδειξη.
Γράφουμε τον αριθμό ν στην κανονική του μορφή $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\varkappa^{\alpha_\varkappa}$ και εφαρμόζουμε διαδοχικά το Θεώρημα 2.3.3.

Παρατήρηση
Το παραπάνω πόρισμα μας δίνει έναν εύκολο τρόπο να υπολογίζουμε γρήγορα το $\varphi(\nu)$ για μεγάλο ν, όπου ο ορισμός γίνεται δύσχρηστος.

Εφαρμογές 2.3

1. Να υπολογισθεί το φ(ν) για τους αριθμούς $\nu = 2, 3, \ldots, 15$.

   Λύση.

   Οι αριθμοί 2, 3, 5, 7, 11, 13 είναι πρώτοι, οπότε φ(2)=1, φ(3)=2, φ(5)=4, φ(7)=6, φ(11)=10, φ(13)=12. Επίσης χρησιμοποιώντας ότι η φ είναι πολλαπλασιαστική συνάρτηση έχουμε ότι:
   $\varphi(6) = \varphi(2)\varphi(3) = 2$, $\varphi(10) = \varphi(2)\varphi(5) = 4$, $\varphi(14) = \varphi(2)\varphi(7) = 6$, $\varphi(15) = \varphi(3)\varphi(5) = 8$.
   Επιπλέον χρησιμοποιώντας το Πόρισμα 2.3.4 προκύπτει ότι $\varphi(4) = 4\left(1 - \frac{1}{2}\right) = 2$, $\varphi(9) = 9\left(1 - \frac{1}{3}\right) = 6$ και $\varphi(8) = 8\left(1 - \frac{1}{2}\right) = 4$.
   Τέλος $\varphi(12) = \varphi(3)\varphi(4) = 4$.

2. Έστω ένας φυσικός αριθμός $\nu > 2$. Να αποδειχθεί ότι το άθροισμα των φυσικών που είναι μικρότεροι του ν και σχετικά πρώτοι μαζί του, δίνεται από τον τύπο $\nu\varphi(\nu)/2$.

   Απόδειξη.

   Προφανώς, αν ο $\kappa < \nu$ είναι σχετικά πρώτος με τον ν, τότε και ο $\nu - \kappa$ είναι επίσης σχετικά πρώτος με τον ν. Έτσι οι αριθμοί που είναι μικρότεροι του ν και σχετικά πρώτοι μαζί του μπορεί να χωριστούν σε $\varphi(\nu)/2$ ζεύγη όπου το άθροισμα των στοιχείων κάθε ζεύγους να ισούται με ν.

3. Για έναν τυχαίο φυσικό ν να αποδειχθεί ότι $\varphi(\nu) \geq \nu/\delta(\nu)$.

   Απόδειξη.

   Έστω $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ η κανονική μορφή του φυσικού ν. Έχουμε το γινόμενο

$$\varphi(\nu)\cdot\delta(\nu) = \nu\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_\kappa}\right)(\alpha_1+1)\ldots(\alpha_\kappa+1).$$

   Άρα

$$\begin{aligned} \varphi(\nu)\cdot\delta(\nu) &\geq \nu\left(\tfrac{1}{2}\right)^\kappa \cdot 2^\kappa \quad \text{ή} \\ \varphi(\nu)\cdot\delta(\nu) &\geq \nu. \end{aligned}$$

4. Να υπολογισθούν οι φυσικοί αριθμοί ν που ικανοποιούν την εξίσωση $\varphi(\nu) = 4\nu/5$.

   Λύση.

   Επειδή ο αριθμός $4\nu/5$ πρέπει να είναι φυσικός είναι φανερό ότι ο ν είναι πολλαπλάσιος του 5, δηλαδή $\nu = 5^{\varkappa} \cdot \mu$ με $(5, \mu) = 1$.
   Αχόμη $\varphi(5^{\varkappa}\mu) = \varphi(5^{\varkappa}) \cdot \varphi(\mu) = 4 \cdot 5^{\varkappa-1} \cdot \mu$ ή $(5^{\varkappa} - 5^{\varkappa-1})\varphi(\mu) = 4 \cdot 5^{\varkappa-1} \cdot \mu$.
   Άρα $4 \cdot 5^{\varkappa-1} \cdot \varphi(\mu) = 4 \cdot 5^{\varkappa-1} \cdot \mu$, δηλαδή $\varphi(\mu) = \mu$.
   Επομένως $\mu = 1$ και $\nu = 5^{\varkappa}$, όπου $\varkappa$ είναι ένας τυχαίος φυσικός.

5. Αν $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{\varkappa}^{\alpha_{\varkappa}}$ είναι ένας φυσικός αριθμός στην κανονική του μορφή, να αποδειχθεί ότι

$$\sigma(\nu) \cdot \varphi(\nu) = \nu^2 \left(1 - \frac{1}{p_1^{\alpha_1+1}}\right)\left(1 - \frac{1}{p_2^{\alpha_2+1}}\right) \dots \left(1 - \frac{1}{p_{\varkappa}^{\alpha_{\varkappa}+1}}\right).$$

   Απόδειξη.

   Γνωρίζουμε ότι

$$\sigma(\nu) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_{\varkappa}^{\alpha_{\varkappa}+1} - 1}{p_{\varkappa} - 1}$$

   και

$$\varphi(\nu) = \nu \left(\frac{p_1 - 1}{p_1}\right)\left(\frac{p_2 - 1}{p_2}\right) \dots \left(\frac{p_{\varkappa} - 1}{p_{\varkappa}}\right).$$

   Άρα $\sigma(\nu) \cdot \varphi(\nu) = \nu \left(\frac{p_1^{\alpha_1+1}-1}{p_1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2}\right) \dots \left(\frac{p_{\varkappa}^{\alpha_{\varkappa}+1}-1}{p_{\varkappa}}\right)$

   ή $\sigma(\nu) \cdot \varphi(\nu) = \nu^2 \left(1 - \frac{1}{p_1^{\alpha_1+1}}\right)\left(1 - \frac{1}{p_2^{\alpha_2+1}}\right) \dots \left(1 - \frac{1}{p_{\varkappa}^{\alpha_{\varkappa}+1}}\right)$.

6. Έστω ν, μ δύο φυσικοί και $\delta = (\nu, \mu)$. Να αποδείξετε ότι $\varphi(\nu\mu) = \varphi(\nu)\varphi(\mu)\delta/\varphi(\delta)$.

   Απόδειξη.

   Έστω ότι οι κανονικές μορφές των φυσικών είναι $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{\varkappa}^{\alpha_{\varkappa}}$ και $\mu = q_1^{\beta_1} q_2^{\beta_2} \dots q_{\tau}^{\beta_{\tau}}$, αντίστοιχα. Από το Πόρισμα 2.3.4 έχουμε ότι

$$\frac{\varphi(\mu\nu)}{\mu\nu} = \frac{\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_{\varkappa}}\right)\left(1 - \frac{1}{q_1}\right) \dots \left(1 - \frac{1}{q_{\tau}}\right)}{(1 - p_1') \dots (1 - p_{\iota}')}$$

όπου $p_1', p_2', \ldots, p_t'$ είναι οι κοινοί πρώτοι παράγοντες των ν και μ. Επιπλέον,

$$\frac{\varphi(\mu\nu)}{\mu\nu} = \frac{\frac{\nu\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_\varkappa}\right)}{\nu} \cdot \frac{\mu\left(1-\frac{1}{q_1}\right)\ldots\left(1-\frac{1}{q_\tau}\right)}{\mu}}{\frac{\delta\left(1-\frac{1}{p_1}\right)\ldots\left(1-\frac{1}{p_t}\right)}{\delta}}$$

δηλαδή

$$\frac{\varphi(\mu\nu)}{\mu\nu} = \frac{\frac{\varphi(\nu)}{\nu} \cdot \frac{\varphi(\mu)}{\mu}}{\frac{\varphi(\delta)}{\delta}}.$$

Άρα $\varphi(\mu\nu) = \varphi(\mu)\varphi(\nu)\delta/\varphi(\delta)$.

7. Να αποδείξετε ότι για κάθε φυσικό $\nu \geq 1$ ισχύει

$$\nu = \sum_{\delta|\nu} \varphi(\delta)$$

όπου το άθροισμα εκτείνεται σε όλους τους φυσικούς διαιρέτες του ν.

Απόδειξη.

Για $\nu = 1$ είναι προφανές ότι

$$\nu = \sum_{\delta|1} \varphi(\delta) = \varphi(1) = 1.$$

Για $\nu > 1$ υποθέτουμε ότι ισχύει για κάθε $\varkappa < \nu$.
Θεωρούμε την κανονική μορφή του αριθμού $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\varkappa^{\alpha_\varkappa}$, οπότε έχουμε ότι

$$\varphi(\nu) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \ldots \cdot \varphi(p_\varkappa^{\alpha_\varkappa}).$$

Άρα

$$\sum_{\delta|\nu} \varphi(\delta) = \sum_{\delta|p_1^{\alpha_1}} \varphi(\delta) \cdot \sum_{\delta|p_2^{\alpha_2}} \varphi(\delta) \cdot \ldots \cdot \sum_{\delta|p_\varkappa^{\alpha_\varkappa}} \varphi(\delta),$$

όπου

$$\sum_{\delta|p_j^{\alpha_j}} \varphi(\delta) = \varphi(1) + \varphi(p_j) + \ldots + \varphi(p_j^{\alpha_j}) \quad \text{ή}$$

$$\sum_{\delta|p_j^{\alpha_j}} \varphi(\delta) = 1 + (p_j - 1) + (p_j^2 - p_j) + \ldots + (p_j^{\alpha_j} - p_j^{\alpha_j - 1}) \text{ ή}$$

$$\sum_{\delta|p_j^{\alpha_j}} \varphi(\delta) = p_j^{\alpha_j}.$$

Επομένως,

$$\sum_{\delta|\nu} \varphi(\delta) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\varkappa^{\alpha_\varkappa} = \nu.$$

8. Βρείτε όλους τους φυσικούς ν για τους οποίους ισχύει $\varphi(\nu) + \sigma(\nu) = 2\nu$.

Λύση.

Προφανώς για $\nu = 1$, έχουμε $\varphi(1) + \sigma(1) = 2$.
Έστω $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\varkappa^{\alpha_\varkappa}$ η κανονική μορφή ενός φυσικού $\nu > 2$.
Τότε έχουμε

$$\nu \cdot \left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_\varkappa}\right) + \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \ldots \frac{p_\varkappa^{\alpha_\varkappa+1} - 1}{p_\varkappa - 1} = 2\nu.$$

Άρα

$$\nu \frac{(p_1-1)\ldots(p_\varkappa-1)}{p_1 p_2 \cdots p_\varkappa} + \frac{\left[(p_1-1)(p_1^{\alpha_1}+\ldots+1)\right]\ldots\left[(p_\varkappa-1)(p_\varkappa^{\alpha_k}+\ldots+1)\right]}{(p_1-1)\ldots(p_\varkappa-1)} = 2\nu \text{ ή}$$

$$\nu \frac{(p_1-1)\ldots(p_\varkappa-1)}{p_1 p_2 \cdots p_\varkappa} + (p_1^{\alpha_1} + \ldots + 1)\ldots(p_\varkappa^{\alpha_\varkappa} + \ldots + 1) = 2\nu \text{ ή}$$

$$\frac{(p_1-1)\ldots(p_\varkappa-1)}{p_1 p_2 \cdots p_\varkappa} + \frac{(p_1^{\alpha_1}+\ldots+1)\ldots(p_\varkappa^{\alpha_\varkappa}+\ldots+1)}{\nu} = 2.$$

Όμως το πηλίκο $(p_1 - 1)\cdots(p_\varkappa - 1)/p_1 p_2 \cdots p_\varkappa$ είναι μικρότερο ή ίσο με $1/2$ και το γινόμενο $(p_1^{\alpha_1} + \cdots + 1)\ldots(p_\varkappa^{\alpha_\varkappa} + \ldots + 1)$ είναι μεγαλύτερο ή ίσο του 2ν, άτοπο.
Άρα μόνο για $\nu = 1$, έχουμε $\varphi(\nu) + \sigma(\nu) = 2\nu$.

Ασκήσεις 2.3

Α' Ομάδα

1. Πόσοι φυσικοί μικρότεροι του 3600 είναι σχετικά πρώτοι ως προς τον αριθμό 3600;

2. Να βρεθούν οι αριθμοί $\varphi(100)$, $\varphi(1000)$, $\varphi(7200)$.

3. Έστω ν και μ δύο φυσικοί τέτοιοι ώστε κάθε πρώτος διαιρέτης του ν να διαιρεί και τον μ. Να αποδειχθεί ότι

$$(\mathrm{i})\varphi(\nu\mu) = \nu\varphi(\mu)\ ,\ (\mathrm{ii})\varphi(\nu^2) = \nu\varphi(\nu).$$

4. Αν ν, δ είναι δύο φυσικοί αριθμοί με $\delta \mid \nu$, τότε $\varphi(\delta) \mid \varphi(\nu)$.

Β' Ομάδα

5. Για ποιους αριθμούς ν ισχύει η σχέση $\varphi(2\nu)=\varphi(\nu)$;

6. Αν ο ν έχει ακριβώς κ διαφορετικούς περιττούς πρώτους παράγοντες, να αποδείξετε ότι $2^\kappa \mid \varphi(\nu)$.

7. Να λυθεί η εξίσωση $\varphi(\nu)=24$.

8. Να αποδείξετε ότι δεν υπάρχει ακέραιος ν τέτοιος ώστε $\varphi(\nu)=14$.

9. Αν $\varphi(\kappa)=\varphi(\nu\kappa)$ για κάποιους αριθμούς ν,κ να αποδείξετε ότι $\nu=2$ και κ=περιττός.

10. Να υπολογισθεί το άθροισμα $\varphi(1) + \varphi(p) + \ldots + \varphi(p^\kappa)$ για ένα τυχαίο πρώτο αριθμό p.

2.4 Τα Θεωρήματα Fermat και Euler

Αν παρατηρήσουμε τη συμπεριφορά του $\alpha^x\,(mod\nu)$ για διάφορες τιμές του x παρατηρούμε ότι συχνά για κάποια τιμή έχουμε $\alpha^\lambda \equiv 1(mod\nu)$. Αυτό είναι αρκετά σημαντικό, καθώς δηλώνει μια περιοδικότητα στη δομή του α^x, δηλαδή $\alpha^{\lambda+\mu} \equiv \alpha^\lambda\alpha^\mu \equiv \alpha^\mu(mod\nu)$. Για παράδειγμα, ας εξετάσουμε τη δύναμη $7^x(mod10)$ για μερικές τιμές του x:

$$\begin{aligned}
7^0 &\equiv 1(mod10)\\
7^1 &\equiv 7(mod10)\\
7^2 &\equiv 49 \equiv 9(mod10)\\
7^3 &\equiv 7^2\cdot 7 \equiv 9\cdot 7 \equiv 3(mod10)\\
7^4 &\equiv 7^3\cdot 7 \equiv 3\cdot 7 \equiv 1(mod10)\\
7^5 &\equiv 7^4\cdot 7 \equiv 1\cdot 7 \equiv 7(mod10)\\
7^6 &\equiv 7^4\cdot 7^2 \equiv 1\cdot 49 \equiv 9(mod10)\\
&\vdots
\end{aligned}$$

δηλαδή τα υπόλοιπα του $7^x(mod10)$ επαναλαμβάνονται περιοδικά με περίοδο 4, παίρνοντας τις τιμές 1, 7, 9, 3.
Αν διαλέγαμε όμως την τιμή α=2, δεν θα είχαμε ποτέ $2^x \equiv 1(mod10)$ αφού ο 2^x είναι άρτιος. Παρ' όλα αυτά, αν μελετήσουμε τις τιμές του $2^x(mod10)$, για $x \geq 1$ παρατηρούμε ότι και εκεί τελικά τα υπόλοιπα επαναλαμβάνονται περιοδικά με περίοδο 4:

$$\begin{aligned}
2^1 &= 2 \quad (mod10)\\
2^2 &\equiv 4 \quad (mod10)\\
2^3 &\equiv 8 \quad (mod10)\\
2^4 &\equiv 6 \quad (mod10)\\
2^5 &= 2 \quad (mod10)\\
2^6 &\equiv 4 \quad (mod10)\\
&\vdots
\end{aligned}$$

Παρατηρούμε, λοιπόν, μια δομή στη μορφή του $\alpha^x(mod\nu)$, η οποία όπως θα δούμε είναι άμεσα συνδεδεμένη με τον αριθμό φ(ν).

Θεώρημα 2.4.1 (Fermat)
Αν p πρώτος και α ακέραιος με $(p, \alpha) = 1$, τότε

$$\alpha^{p-1} \equiv 1(modp).$$

Απόδειξη.
Προκύπτει άμεσα ως ειδική περίπτωση του θεωρήματος του Euler που ακολουθεί.

Θεώρημα 2.4.2 (Euler)
Αν α, m ακέραιοι με $(\alpha, m) = 1$, τότε

$$\alpha^{\varphi(m)} \equiv 1(modm)$$

όπου $\varphi(m)$ είναι η συνάρτηση του Euler.
Απόδειξη.
Για $m = 2$ προφανώς ισχύει, αφού αν $(\alpha, 2) = 1$ ο α είναι περιττός. Για $m \geq 3$, ας θεωρήσουμε τους $\varphi(m)$ αριθμούς

$$r_1, r_2, \ldots, r_{\varphi(m)}$$

που είναι σχετικά πρώτοι με το m. Αν πολλαπλασιάσουμε με το $\alpha(modm)$ παίρνουμε τους αριθμούς

$$\alpha \cdot r_1, \alpha \cdot r_2, \ldots, \alpha \cdot r_{\varphi(m)}(modm).$$

Επειδή $(\alpha, m) = 1$, ούτε ο α ούτε ο r_i έχουν παράγοντα τον αριθμό m, οπότε ο αr_i είναι σχετικά πρώτος με τον m για κάθε i. Όμως οι αριθμοί $r_1, r_2, \ldots, r_{\varphi(m)}$ είναι όλοι οι σχετικά πρώτοι του $m(modm)$, οπότε $\alpha r_i = r_j$. Επίσης, αποκλείεται $\alpha r_i \equiv \alpha r_j(modm)$ για κάποιους r_i, r_j, αφού τότε θα είχαμε $r_i \equiv r_j(modm)$ από το νόμο της διαγραφής, αφού $(\alpha, m) = 1$, άτοπο.
Έτσι οι αριθμοί $\alpha \cdot r_1, \alpha \cdot r_2, \ldots, \alpha \cdot r_{\varphi(m)}(modm)$ είναι οι ίδιοι με τους $r_1, r_2, \ldots, r_{\varphi(m)}(modm)$, με διαφορετική διάταξη. Άρα

$$\begin{aligned}
(\alpha r_1)(\alpha r_2)\ldots(\alpha r_{\varphi(m)}) &\equiv r_1 r_2 \ldots r_{\varphi(m)}(modm) \quad \text{ή} \\
\alpha^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} &\equiv r_1 r_2 \ldots r_{\varphi(m)}(modm) \quad \text{ή} \\
\alpha^{\varphi(m)} &\equiv 1(modm), \quad \text{αφού} (m, r_i) = 1 \text{ για κάθε } i.
\end{aligned}$$

Σχόλιο
Για δύο σχετικά πρώτους ακεραίους α, m το $\varphi(m)$ δεν είναι απαραίτητα η ελάχιστη δύναμη με την ιδιότητα: $\alpha^{\varphi(m)} \equiv 1(modm)$. Η ελάχιστη αυτή δύναμη e λέγεται **εκθέτης** του α ως προς $modm$.

Πόρισμα 2.4.3
Αν p πρώτος και α ακέραιος με $(p, \alpha) = \delta \geq 1$, τότε

$$\alpha^p \equiv \alpha(modp).$$

Απόδειξη.
Αν $(p, \alpha) = 1$, τότε από το Θεώρημα Fermat $\alpha^{p-1} \equiv 1(modp)$, άρα $\alpha^p \equiv \alpha(modp)$. Αν $(p, \alpha) > 1$ τότε $p \mid \alpha$, άρα $\alpha^p \equiv \alpha \equiv 0(modp)$.

Τα θεωρήματα Fermat και Euler αποτελούν ένα από τα πιο όμορφα αποτελέσματα της Θεωρίας των Αριθμών, λόγω της καθολικότητάς τους, δηλαδή της εφαρμογής τους στο σύνολο των φυσικών αριθμών.
Ένα πραγματικά "ξεχασμένο" θεώρημα είναι το θεώρημα Lucas, που είναι το πραγματικό αντίστροφο του θεωρήματος του Fermat:

Θεώρημα 2.4.4 (Lucas)
Αν $p \mid \alpha^x - 1$ για $x = p - 1$, αλλά όχι για $x < p - 1$, τότε ο p είναι πρώτος.

Εφαρμογές 2.4

1. Ποιο είναι το τελευταίο ψηφίο του 2^{400};

   Λύση.

   Από το Θεώρημα Fermat έχουμε $2^4 \equiv 1(mod5)$, άρα $2^{400} \equiv 1(mod5)$ κι επειδή ο αριθμός 2^{400} είναι άρτιος, καταλήγουμε ότι $2^{400} \equiv 6(mod10)$, δηλαδή το ζητούμενο ψηφίο είναι το 6.

2. Βρείτε τα δύο τελευταία ψηφία του αριθμού 3^{400}.

   Λύση.

   Από το Θεώρημα Euler γνωρίζουμε ότι

   $$3^{20} \equiv 1(mod25),$$

   αφού $\varphi(25)=20$. Επιπλέον $3^2 \equiv 1(mod4)$, άρα

   $$3^{20} \equiv 1(mod4)$$

   και αφού $(4, 25) = 1$ καταλήγουμε ότι

   $$\begin{aligned} 3^{20} &\equiv 1(mod100) \quad \acute{\eta} \\ 3^{400} &\equiv 1(mod100). \end{aligned}$$

   Επομένως τα δύο τελευταία ψηφία του 3^{400} είναι 01.

3. Βρείτε το υπόλοιπο της διαίρεσης του 41^{75} διά του 3.

   Λύση.

   Επειδή $(41, 3) = 1$, από το Θεώρημα Fermat έχουμε ότι

   $$\begin{aligned} 41^2 &\equiv 1(mod3) \quad \acute{\eta} \\ 41^{74} &\equiv 1(mod3) \quad \acute{\eta} \\ 41^{75} &\equiv 41(mod3) \quad \acute{\eta} \\ 41^{75} &\equiv 2(mod3). \end{aligned}$$

   Άρα το υπόλοιπο της διαίρεσης του 41^{75} δια του 3 είναι υ=2.

4. Αν α και μ είναι δύο φυσικοί αριθμοί με $(\alpha, \mu) = (\alpha - 1, \mu) = 1$, να αποδειχθεί ότι $1 + \alpha + \alpha^2 + \ldots + \alpha^{\varphi(\mu)-1} \equiv 0(mod\mu)$.

   Απόδειξη.

   Από το Θεώρημα Euler έχουμε

   $$\alpha^{\varphi(\mu)} \equiv 1(mod\mu) \quad \text{ή}$$
   $$\alpha^{\varphi(\mu)} - 1 \equiv 0(mod\mu) \quad \text{ή}$$
   $$(\alpha - 1)(\alpha^{\varphi(\mu)-1} + \ldots + \alpha^2 + \alpha + 1) \equiv 0(mod\mu).$$

   Αφού $(\alpha - 1, \mu) = 1$ είναι προφανές ότι $\alpha - 1 \not\equiv 0(mod\mu)$ και

   $$\alpha^{\varphi(\mu)-1} + \ldots + \alpha^2 + \alpha + 1 \equiv 0(mod\mu).$$

5. Να αποδειχθεί ότι για κάθε τυχαίο φυσικό ν ισχύει $30 \mid (\nu^5 - \nu)$ και $42 \mid (\nu^7 - \nu)$.

   Απόδειξη.

   Ο φυσικός $\nu^5 - \nu$ γράφεται

   $$\nu^5 - \nu = \nu(\nu^4 - 1) = \nu(\nu - 1)(\nu + 1)(\nu^2 - 1)$$

   και $6 \mid [\nu(\nu - 1)(\nu + 1)]$.
   Επιπλέον από το Θεώρημα Fermat ο πρώτος αριθμός 5 διαιρεί τέλεια τον $\nu^5 - \nu$.
   Αφού (5,6)=1, είναι φανερό ότι $30 \mid (\nu^5 - \nu)$.

   Ο φυσικός $\nu^7 - \nu$ γράφεται

   $$\nu^7 - \nu = \nu(\nu^6 - 1) = \nu(\nu^3 - 1)(\nu^3 + 1) \quad \text{ή}$$
   $$\nu^7 - \nu = \nu(\nu + 1)(\nu - 1)(\nu^2 + \nu + 1)(\nu^2 - \nu + 1)$$

   όπου $6 \mid [\nu(\nu - 1)(\nu + 1)]$ και από το Θεώρημα Fermat, ο πρώτος αριθμός 7 διαιρεί τέλεια τον $\nu^7 - \nu$.
   Αφού (6,7)=1, είναι προφανές ότι $42 \mid (\nu^7 - \nu)$.

Ασκήσεις 2.4

Α' Ομάδα

1. Αν ν ένας περιττός φυσικός και $\kappa \geq 1$ να αποδειχθεί ότι

$$\nu^{2^\kappa} \equiv 1(mod 2^{\kappa+2}).$$

2. Έστω τρεις φυσικοί ν, μ και δ και ένας πρώτος αριθμός p τέτοιος ώστε $\nu^\delta \equiv 1(mod p^\mu)$.
   Να αποδειχθεί ότι $\nu^{p\delta} \equiv 1(mod p^{\mu+1})$.

3. Να αποδείξετε ότι για κάθε ακέραιο ν,
   (α) Το 3 διαιρεί τον $\nu^3 - \nu$,
   (β) Το 5 διαιρεί τον $\nu^5 - \nu$,
   (γ) Το 7 διαιρεί τον $\nu^7 - \nu$,
   (δ) Το 11 διαιρεί τον $\nu^{11} - \nu$,
   (ε) Το 13 διαιρεί τον $\nu^{13} - \nu$.

4. Να αποδείξετε ότι για κάθε ζεύγος φυσικών αριθμών (μ, ν) ο αριθμός $\mu\nu(\mu^{60} - \nu^{60})$ διαιρείται με το 56786730.
   (Υπόδειξη: $56786730 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 31 \cdot 61$)

5. Να αποδείξετε ότι $91 \mid (\nu^{37} - \nu)$ για κάθε φυσικό ν.

Β' Ομάδα

6. Να αποδείξετε ότι το σύνολο των ακεραίων της μορφής $2^\kappa - 3$, όπου $\kappa = 2, 3, 4, \ldots$ περιέχει ένα υποσύνολο με άπειρα στοιχεία τέτοιο ώστε κάθε δύο στοιχεία του να είναι πρώτοι μεταξύ τους.
   (13η ΔΜΟ, 1971, Τσεχοσλοβακία)

7. Αν $p \neq q$ δύο περιττοί πρώτοι, να αποδείξετε ότι

$$p^{q-1} + q^{p-1} \equiv 1(mod pq).$$

8. Να αποδείξετε ότι $\alpha^{\varphi(\beta)} + \beta^{\varphi(\alpha)} \equiv 1(mod \alpha\beta)$, όπου α, β ακέραιοι με $(\alpha, \beta) = 1$.

9. Αν $(\alpha, \beta) = 1$ για κάποιον ακέραιο α, να αποδείξετε ότι

$$\alpha^2 \equiv 1(mod 24).$$

10. Αν $\nu \geq 1$ περιττός, να αποδείξετε ότι ο αριθμός

$$\frac{2^{\nu!} - 1}{\nu}$$

είναι ακέραιος.

2.5 Το Θεώρημα Wilson

Το ακόλουθο αποτέλεσμα αποτελεί ένα από τα λίγα καθολικά κριτήρια πρώτων αριθμών, το οποίο ωστόσο είναι ιδιαίτερα δύσχρηστο λόγω των μεγάλων αριθμών που προκύπτουν.

Θεώρημα 2.5.1 (Wilson)
Ο φυσικός $p > 2$ είναι πρώτος αν και μόνο αν

$$(p-1)! \equiv -1(mod p).$$

Απόδειξη.
Αν ο αριθμός p είναι πρώτος γνωρίζουμε ότι οι αριθμοί $2, 3, \ldots, p-2$ αποτελούν ζεύγη αντιστρόφων $mod p$, οπότε

$$2 \cdot 3 \cdot \ldots (p-2) \equiv 1(mod p).$$

Έτσι $(p-1)! = 2 \cdot 3 \cdot \ldots \cdot (p-2)(p-1) \equiv -1(mod p)$.
Αντίστροφα, έστω ότι $(p-1)! \equiv -1(mod p)$ και ο p είναι σύνθετος.
Ο p δεν μπορεί να είναι ίσος με 4, αφού $(4-1)! = 6 \not\equiv -1(mod 4)$.
Έστω $p > 4$. Τότε, αφού p=σύνθετος, $p = \alpha\beta$ για κάποιους α, β με $1 < \alpha, \beta < p$. Οι α, β θα εμφανίζονται ως όροι στο παραγοντικό $(p-1)!$, οπότε $(p-1)! \equiv 0(mod p)$, εκτός αν ο p είναι τετράγωνο πρώτου, δηλαδή $p = q^2$, q πρώτος. Αλλά και σε αυτή την περίπτωση $(p-1)! \equiv 0(mod p)$, αφού ο $2q$ εμφανίζεται στο γινόμενο, άτοπο. Άρα ο p είναι πρώτος.

Ασκήσεις 2.5

Α' Ομάδα

1. Αν ο p είναι ένας περιττός πρώτος, να αποδείξετε ότι
$$2(p-3)! \equiv -1(mod p).$$

2. Αν ο p είναι ένας πρώτος της μορφής $p \equiv 1(mod 4)$ να αποδείξετε ότι
$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1(mod p).$$

3. Αν ο p είναι ένας πρώτος της μορφής $p \equiv 3(mod 4)$ να αποδείξετε ότι
$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1(mod p).$$

Β' Ομάδα

4. Έστω $p > 2$ ένας πρώτος αριθμός και έστω $(\alpha_1, \alpha_2, \ldots, \alpha_p)$ και $(\beta_1, \beta_2, \ldots, \beta_p)$ δύο μεταθέσεις των αριθμών $(0, 1, 2, \ldots, p-1)$. Για κάθε $i = 1, 2, \ldots, p$ ορίζουμε γ_i το υπόλοιπο της διαίρεσης $\alpha_i\beta_i$ με το p. Να αποδείξετε ότι οι αριθμοί $(\gamma_1, \gamma_2, \ldots, \gamma_p)$ δεν αποτελούν μία μετάθεση των αριθμών $(0, 1, 2, \ldots, p-1)$.

5. Να βρείτε όλους τους φυσικούς $\nu > 1$ για τους οποίους το σύνολο $\{1!, 2!, \ldots, \nu!\}$ είναι ισότιμο με το $\{0, 1, 2, \ldots, \nu-1\} modulo\ \nu$.

2.6 Εφαρμογές των Ισοτιμιών

2.6.1 Κριτήρια Διαιρετότητας

Στο προηγούμενο κεφάλαιο είδαμε μερικά κριτήρια διαιρετότητας, δηλαδή τρόπους με τους οποίους μπορούμε να βρούμε εύκολα αν ένας αριθμός διαιρείται με ένα φυσικό. Ας δούμε πώς μπορούμε να κατασκευάσουμε κριτήρια διαιρετότητας για οποιονδήποτε διαιρέτη.
Ας εξετάσουμε για παράδειγμα την περίπτωση διαίρεσης με το 7. Ας θεωρήσουμε τη γραφή του αριθμού N, στο δεκαδικό σύστημα αρίθμησης:

$$N = \alpha_\nu \cdot 10^\nu + \alpha_{\nu-1} \cdot 10^{\nu-1} + \ldots + \alpha_2 \cdot 10^2 + \alpha_1 \cdot 10 + \alpha_0$$

όπου $\alpha_\nu, \alpha_{\nu-1}, \ldots, \alpha_0$ είναι τα ψηφία του αριθμού N.
Θέλουμε να εξετάσουμε αν $N \equiv 0(mod 7)$ ή όχι. Παρατηρούμε ότι

$$\begin{aligned} 10^0 &\equiv 1(mod 7) \\ 10^1 &\equiv 3(mod 7) \\ 10^2 &\equiv 2(mod 7) \\ 10^3 &\equiv 6(mod 7) \\ 10^4 &\equiv 4(mod 7) \\ 10^5 &\equiv 5(mod 7) \\ 10^6 &\equiv 1(mod 7) \end{aligned}$$

δηλαδή όλα τα υπόλοιπα επαναλαμβάνονται περιοδικά με περίοδο 6.
Στην περίπτωσή μας κάτι τέτοιο εξασφαλίζεται από το θεώρημα του Fermat, αφού ο 7 είναι πρώτος συνεπώς $10^6 \equiv 1(mod 7)$.

Για παράδειγμα, αν ο N είναι επταψήφιος

$$N = \overline{\alpha_6\alpha_5\alpha_4\alpha_3\alpha_2\alpha_1\alpha_0}$$

τότε $N \equiv 1 \cdot \alpha_6 + 5 \cdot \alpha_5 + 4 \cdot \alpha_4 + 6 \cdot \alpha_3 + 2 \cdot \alpha_2 + 3 \cdot \alpha_1 + \alpha_0(mod 7)$.
Το άθροισμα του δεύτερου μέλους είναι μικρότερο του N οπότε είναι ευκολότερο να ελεγχθεί αν είναι πολλαπλάσιο του 7 ή όχι από ό,τι ο N.

Το κριτήριο αυτό γίνεται πιο εύχρηστο αν παρατηρήσουμε ότι

$$\begin{aligned} 10^3 &\equiv 6 \equiv -1(mod 7) \\ 10^4 &\equiv 4 \equiv -3(mod 7) \\ 10^5 &\equiv 5 \equiv -2(mod 7), \end{aligned}$$

οπότε το κριτήριο διαιρετότητας μπορεί να διατυπωθεί ως εξής:

"Χωρίζουμε τα ψηφία του αριθμού N σε εξάδες από δεξιά προς τα αριστερά. Στη συνέχεια πολλαπλασιάζουμε τον τελευταίο (προς τα δεξιά) αριθμό κάθε εξάδας με το 1, τον προτελευταίο με το 3, τον επόμενο με 2 και τους υπόλοιπους τρεις με -1, -3, -2 αντίστοιχα. Προσθέτουμε τα γινόμενα. Ο αριθμός N διαιρείται με τον 7 αν και μόνο αν το σχηματιζόμενο άθροισμα διαιρείται με το 7".

Με παρόμοιο τρόπο μπορούμε να βρούμε κριτήρια διαιρετότητας για οποιονδήποτε διαιρέτη.

2.6.2 Η ημέρα της εβδομάδας

Ο Ιούλιος Καίσαρας, προσαρμόζοντας το Αιγυπτιακό ημερολόγιο, δημιούργησε το 45 π.Χ. το ημερολόγιο με τους 12 μήνες και τις 365 ημέρες που γνωρίζουμε, το **Ιουλιανό Ημερολόγιο**, δίνοντας μάλιστα το όνομά του σε ένα μήνα.
Επειδή γνώριζαν ότι ένας χρόνος έχει περίπου $365\frac{1}{4}$ ημέρες, καθιερώθηκε επίσης το δίσεκτο έτος με μία επιπλέον ημέρα κάθε τέσσερα χρόνια.
Παρ' όλα αυτά, οι αστρονόμοι αργότερα διαπίστωσαν ότι η διάρκεια ενός έτους είναι περίπου 365,2422 ημέρες, δηλαδή λίγο λιγότερο από το $365\frac{1}{4}$ του Ιουλιανού ημερολογίου. Αυτό έχει σαν συνέπεια καθε 400 χρόνια να χρειάζεται να προσθέσουμε μόνο 97 δίσεκτα έτη και όχι 100. Ο πάπας Γρηγόριος ο 13ος, το 1582, για να διορθώσει αυτή την ατέλεια, καθιέρωσε το **Γρηγοριανό Ημερολόγιο**, σύμφωνα με το οποίο ένα έτος είναι δίσεκτο αν διαιρείται με το 4, εκτός από τα έτη των αιώνων (δηλαδή αυτά που διαιρούνται με το 100) τα οποία είναι δίσεκτα μόνο αν διαιρούνται με 400. Έτσι εξασφαλίζονται 97 δίσεκτα έτη κάθε 400 χρόνια. Επίσης για να διορθωθεί αυτή η παράλειψη από την εποχή του Ιούλιου Καίσαρα προστέθηκαν 10 ημέρες, δηλαδή η 5 Οκτωβρίου 1582 μετονομάσθηκε σε 15 Οκτωβρίου 1582.
Το Γρηγοριανό ημερολόγιο είναι αυτό που χρησιμοποιείται σήμερα στις περισσότερες χώρες του Δυτικού κόσμου, ωστόσο η αλλαγή αυτή δεν έγινε παντού το 1582. Στη Βρετανία (και στις τωρινές ΗΠΑ οι οποίες δεν είχαν ανεξαρτητοποιηθεί ακόμη) το ημερολόγιο άλλαξε το 1752, οπότε χρειάστηκαν να προστεθούν 11 ημέρες, στην Ιαπωνία το 1873, στη Σοβιετική Ένωση το 1917, ενώ στην Ελλάδα το 1923, οπότε προστέθηκαν

13 ημέρες, αφού τα έτη 1700, 1800, 1900 δεν είναι δίσεκτα σύμφωνα με το νέο ημερολόγιο.

Ας προσπαθήσουμε να βρούμε ένα τύπο που να μας δίνει τη ημέρα της εβδομάδας για οποιαδήποτε ημέρα του Γρηγοριανού Ημερολογίου. Επειδή οι ημέρες επεναλαμβάνονται κάθε επτά, είναι φανερό ότι πρέπει να χρησιμοποιήσουμε modulo 7.
Ας συμβολίσουμε τις ημέρες με τους αριθμούς 0 έως 6 αρχίζοντας από την Κυριακή $= 0$ έως Σάββατο $= 6$. Επίσης, έστω H η ημέρα, M ο μήνας, A ο αιώνας και E το έτος του αιώνα της ζητούμενης ημερομηνίας. Για παράδειγμα για την 1η Ιανουαρίου 1999 έχουμε H=1, M=1, A=19, E=99.
Επειδή η δίσεκτη ημέρα προστίθεται στις 29 Φεβρουαρίου, ας προσπαθήσουμε να βρούμε ένα τύπο για την 1η Μαρτίου οποιουδήποτε έτους ε, την οποία ας συμβολίσουμε με x_ε. Αν δεν υπήρχαν δίσεκτα έτη, επειδή $365 \equiv 1(mod 7)$ η 1η Μαρτίου θα μετατοπιζόταν μία ημέρα κάθε χρόνο, δηλαδή

$$x_\varepsilon \equiv x_d + (\varepsilon - d)(mod 7)$$

όπου x_d είναι η ημέρα της 1ης Μαρτίου του έτους d, η οποία χρησιμοποιείται ως ημέρα αναφοράς και είναι γνωστή π.χ. από ένα ημερολόγιο. Για παράδειγμα, μπορούμε να θέσουμε $d = 1600$, $x_d = 3$, αφού η 1η Μαρτίου 1600 ήταν Τετάρτη.
Έτσι έχουμε:

$$x_\varepsilon \equiv 3 + (\varepsilon - 1600)(mod 7) \text{ ή}$$

$$x_\varepsilon \equiv 3 + (100A + E - 1600)(mod 7).$$

Αν υποθέσουμε ότι τα δίσεκτα έτη επαναλαμβάνονται περιοδικά κάθε 4 χρόνια, θα πρέπει να προσθέσουμε

$$\left[\frac{1}{4}(100A + E - 1600)\right] = 25A - 400 + \left[\frac{1}{4}E\right]$$

όπου η αγκύλη συμβολίζει το ακέραιο μέρος.

Αυτό έχει ως αποτέλεσμα την άυξηση του x_ε κατά 1 κάθε φορά που συναντάμε ένα δίσεκτο έτος. Από αυτά τα "δίσεκτα" έτη θα πρέπει να αφαιρέσουμε τα έτη των αιώνων τα οποία δεν είναι πάντα δίσεκτα και τα οποία είναι $A - 16$ στο πλήθος και στη συνέχεια να προσθέσουμε

$$\left[\frac{1}{4}(A - 16)\right] = \left[\frac{1}{4}A\right] - 4$$

για όσα έτη αιώνων είναι πράγματι δίσεκτα. Έτσι καταλήγουμε στον εξής τύπο για την ημέρα της 1ης Μαρτίου οποιουδήποτε έτους $\varepsilon = 100A + E$ του Γρηγοριανού Ημερολογίου:

$$x_\varepsilon \equiv 3+(100A+E-1600)+25A-400+\left[\frac{1}{4}E\right]-(A-16)+\left[\frac{1}{4}A\right]-4(mod7)$$

$$\acute{\eta}\ x_\varepsilon \equiv 3-2A+E+\left[\frac{1}{4}A\right]+\left[\frac{1}{4}E\right](mod7).$$

Τέλος, αρκεί να υπολογίσουμε πόσες ημέρες μετά την 1η Μαρτίου έχουμε μία τυχαία ημερομηνία.

Επειδή ο Μάρτιος έχει $31 \equiv 3(mod7)$ ημέρες, θα πρέπει να προσθέσουμε 3 ημέρες για να πάρουμε την ημέρα της 1ης Απριλίου αν γνωρίζουμε την 1η Μαρτίου, 5 μέρες (αφού ο Απρίλιος έχει 30 μέρες) για την 1η Μαΐου κ.λπ., καταλήγοντας στον παρακάτω πίνακα:

Μάρτιος	0	*Σεπτέμβριος*	16
Απρίλιος	3	*Οκτώβριος*	18
Μάιος	5	*Νοέμβριος*	21
Ιούνιος	8	*Δεκέμβριος*	23
Ιούλιος	10	*Ιανουάριος*	26
Αύγουστος	13	*Φεβρουάριος*	29

Παρατηρούμε ότι οι αριθμοί αυτοί δεν αποτελούν αριθμητική πρόοδο, όμως αυξάνονται περίπου κατά 2,6 κάθε μήνα. Αν δοκιμάσουμε τον τύπο $[2,6(M-3)]$ –αφού ο Μάρτιος είναι ο τρίτος μήνας–διαπιστώνουμε ότι δε δίνει όλες τις σωστές τιμές. Με τη μικρή διόρθωση

$$[2,6(M-3)+0,4] = \left[\frac{1}{5}(13M-37)\right]$$

παίρνουμε τις σωστές τιμές και για τους 12 μήνες.

Έχοντας βρει την ημέρα της 1ης του μηνός που ενδιαφερόμαστε, αρκεί να προσθέσουμε τον αριθμό της μέρας που θέλουμε. Η ζητούμενη μέρα της εβδομάδας δίνεται λοιπόν από τον τύπο:

$$3-2A+E+\left[\frac{1}{4}A\right]+\left[\frac{1}{4}E\right]+\left[\frac{1}{5}(13M-37)\right]+H(mod7)$$

$$\text{ή} \quad \left[\frac{1}{4}A\right] + \left[\frac{1}{4}E\right] + \left[\frac{1}{5}(13M - 37)\right] - 2A + E + H + 3(mod 7)$$

Για παράδειγμα για την 1η Ιανουαρίου 1999 έχουμε:

$$\left[\frac{1}{4} \cdot 19\right] + \left[\frac{1}{4} \cdot 99\right] + \left[\frac{1}{5}(13 \cdot 1 - 37)\right] - 2 \cdot 19 + 99 + 1 + 3 = 89 \equiv 5(mod 7).$$

Άρα η ημέρα αυτή είναι Παρασκευή.

Εφαρμογές 2.6

1. Να εξετάσετε αν ο αριθμός 12345678905 διαιρείται με το 7.

   Λύση.

   Χωρίζουμε τον αριθμό σε εξάδες

$$\begin{array}{rrrrrr|rrrrrr} 1 & 2 & 3 & 4 & 5 & & 6 & 7 & 8 & 9 & 0 & 5 \\ -3 & -1 & 2 & 3 & 1 & & -1 & -3 & -1 & 2 & 3 & 1 \end{array}$$

   Το άθροισμα των γινομένων είναι:
   $1(-3)+2(-1)+3\cdot 2+4\cdot 3+5\cdot 1+6(-2)+7(-3)+8(-1)+$
   $+9\cdot 2+0\cdot 3+5\cdot 1=0$, το οποίο διαιρείται με το 7.
   Έτσι ο αρχικός αριθμός διαιρείται με το 7.

2. Να βρείτε κριτήρια διαιρετότητας για το 9.

   Λύση.

   Έχουμε

$$\begin{aligned} 10^0 &\equiv 1(mod 9) \\ 10^1 &\equiv 1(mod 9) \\ 10^2 &\equiv 1(mod 9) \\ &\vdots \end{aligned}$$

   δηλαδή οι συντελεστές του κριτηρίου διαιρετότητας είναι όλοι 1. Το κριτήριο λοιπόν για διαίρεση με το 9 είναι να πολλαπλασιάσουμε κάθε ψηφίο του αριθμού με το 1, να προσθέσουμε τα αποτελέσματα και να εξετάσουμε αν ο σχηματιζόμενος αριθμός διαιρείται με το 9. Αυτό είναι ακριβώς το κριτήριο που είδαμε στο 1ο Κεφάλαιο.

Γενικές Ασκήσεις 2ου Κεφαλαίου

1. Να αποδείξετε ότι ο αριθμός $\nu^2 + 3\nu + 5$ δεν διαιρείται με το 121 για κάθε τιμή του ν.

2. Για κάθε φυσικό $x > 0$ θεωρούμε την ακολουθία

$$A_\nu = \sqrt{x + \sqrt{x + \ldots + \sqrt{x}}}$$

όπου το πλήθος των τετραγωνικών ριζών είναι ν. Αν είναι γνωστό ότι η ακολουθία A_ν τείνει σε κάποιο όριο καθώς $\nu \to \infty$, να βρείτε για ποιες τιμές του x το όριο αυτό είναι ακέραιος. Επίσης να αποδείξετε ότι αν ο x είναι περιττός τότε το όριο αυτό είναι άρρητος.

3. Να λυθεί η εξίσωση $2^x - 3^y = 7$, όπου x, y ακέραιοι με $x, y \geq 1$.

4. Να αποδείξετε ότι υπάρχουν άπειροι φυσικοί οι οποίοι δε μπορούν να γραφούν ως άθροισμα λιγότερων από δέκα τετραγώνων περιττών φυσικών.

5. Έστω α/β ένα κλάσμα με α, β φυσικούς, $\beta \geq 2$, $(\alpha, \beta) = 1$ και $(\beta, 3) = 1$. Να αποδείξετε ότι υπάρχει κλάσμα της μορφής

$$\frac{\nu}{3^\kappa - 1}$$

όπου ν, κ φυσικοί, το οποίο να είναι ίσο με το αρχικό.

6. Ο Διεθνής Τυποποιημένος Αριθμός Βιβλίου ISBN (International Standard Book Number) είναι ένας δεκαψήφιος αριθμός που αναγράφεται στα περισσότερα βιβλία και περιέχει πληροφορίες για την προέλευση του βιβλίου (τα πρώτα 1–3 ψηφία φανερώνουν τη χώρα ή τη γεωγραφική περιοχή που τυπώθηκε το βιβλίο, τα επόμενα 2–5 τον εκδότη και τα επόμενα ως το ένατο, έναν αριθμό που δίνει ο εκδότης στο βιβλίο).
Το τελευταίο ψηφίο καλείται ψηφίο ελέγχου και "ελέγχει" την ορθότητα των πρώτων εννέα αριθμών.

Αν τα ψηφία του ISBN ενός βιβλίου είναι $\alpha_{10}, \alpha_9, \alpha_8, \ldots, \alpha_1$ τότε το ψηφίο ελέγχου επιλέγεται έτσι ώστε

$$\sum_{\varkappa=1}^{10} \varkappa\alpha_\varkappa \equiv 0(mod 11).$$

(Στην περίπτωση που το τελευταίο "ψηφίο" του ISBN είναι το γράμμα "X" τότε αυτό σημαίνει ότι $\alpha_1 = 10$).
(i) Να επαληθεύσετε ότι οι παρακάτω ISBN είναι σωστοί:

$$9600606161, \quad 185326086X.$$

(ii)Να αποδείξετε ότι το ψηφίο ελέγχου θα "πιάσει" ένα λάθος στην περίπτωση που

(α) κατά λάθος αλλάξαμε ένα ψηφίο του αριθμού,

(β) αντιστρέψαμε τη σειρά δύο γειτονικών ψηφίων (π.χ. 67 αντί 76).

7. Έστω $\alpha > 3$ ένας περιττός φυσικός. Να αποδείξετε ότι για κάθε φυσικό $\nu \geq 1$ ο αριθμός $\alpha^{2^\nu} - 1$ έχει τουλάχιστον $\nu + 1$ διαφορετικούς πρώτους παράγοντες.

8. Αν οι x, y είναι ρητοί τέτοιοι ώστε

$$\varepsilon\varphi\pi x = y$$

να αποδείξετε ότι $x = \frac{\varkappa}{4}$ όπου $\varkappa$ ακέραιος με $\varkappa \equiv 2(mod 4)$.

9. Θεωρούμε τον αριθμό 4444^{4444} γραμμένο στο δεκαδικό σύστημα και έστω A το άθροισμα των ψηφίων του. Έστω B το άθροισμα των ψηφίων του A. Να βρείτε το άθροισμα των ψηφίων του B. (17η ΔΜΟ, 1975 Βουλγαρία).

10. Να βρείτε κριτήρια διαιρετότητας για διαίρεση με τους αριθμούς 11, 13, 1000.

11. Να αποδείξετε ότι $p \mid (\alpha^p + (p-1)!\alpha)$ όπου p περιττός πρώτος και α ακέραιος με $(\alpha, p) = 1$.

12. Αν ο αριθμός p είναι πρώτος να αποδείξετε ότι $\binom{2p}{p} \equiv 2(mod p)$.

13. Έστω p ένας πρώτος αριθμός και α, ν τέτοιοι ώστε

$$2^p + 3^p = \alpha^\nu.$$

Να αποδείξετε ότι $\nu = 1$.

14. Αν α, β ακέραιοι και p περιττός πρώτος τέτοιος ώστε

$$\alpha^p \equiv \beta^p (mod p),$$

να αποδείξετε ότι

$$\alpha^p \equiv \beta^p (mod p^2).$$

Κεφάλαιο 3

Ισοτιμίες Ανώτερου Βαθμού

Εισαγωγή

Μία από τις σύγχρονες κατευθύνσεις της έρευνας στη Θεωρία των Αριθμών είναι η σύνδεση των γραμμικών μορφών–που μελετήσαμε στα προηγούμενα κεφάλαια, όπως με τη γραμμική ισοτιμία–με μορφές ανώτερης τάξης. Το πρώτο βήμα στην κατεύθυνση αυτή είναι η προσπάθεια επίλυσης ισοτιμιών ανώτερης τάξης. Αναζητούμε δηλαδή τις ακέραιες λύσεις της ισοτιμίας $f(x) \equiv 0(mod v)$, όπου $f(x)$ είναι ένα πολυώνυμο με ακέραιους συντελεστές.
Ας μελετήσουμε πρώτα την απλούστερη ισοτιμία δεύτερου βαθμού:
$x^2 \equiv a(mod p)$, όπου p πρώτος αριθμός.

3.1 Τετραγωνικά Κατάλοιπα

Καταρχήν παρατηρούμε ότι η ισοτιμία $x^2 \equiv \alpha(mod p)$, όπου p πρώτος, δεν έχει πάντοτε λύσεις. Για παράδειγμα, έχουμε δει ότι το τετράγωνο οποιουδήποτε ακεραίου είναι 0 ή 1 *modulo* 3. Έτσι η ισοτιμία $x^2 \equiv 2(mod 3)$ δεν έχει λύσεις στους ακεραίους.

Επίσης η περίπτωση $p = 2$ είναι αρκετά απλή. Γνωρίζουμε ότι το x^2 είναι περιττός ή άρτιος αν και μόνο αν το x είναι περιττός ή άρτιος αντίστοιχα. Έτσι η εξίσωση $x^2 \equiv 0(mod 2)$ έχει λύση όλους τους άρτιους, ενώ η $x^2 \equiv 1(mod 2)$ τους περιττούς.

Ας εξετάσουμε την περίπτωση $p > 2$. Το πλήθος των λύσεων μίας τέτοιας ισοτιμίας προσδιορίζεται από το ακόλουθο θεώρημα.

Θεώρημα 3.1.1
Αν $p > 2$, $(\alpha, p) = 1$ και η ισοτιμία $x^2 \equiv a(modp)$ έχει λύσεις,τότε θα έχει ακριβώς δύο λύσεις $(modp)$.
Απόδειξη.
Έστω x_1 μία λύση της ισοτιμίας. Τότε προφανώς η $-x_1$ είναι επίσης λύση, αφού επαληθεύει την ισοτιμία. Επιπλέον, η $-x_1$ είναι διαφορετική λύση από την $x_1(modp)$, αφού αν ήταν $x_1 \equiv -x_1(modp)$ τότε $2x_1 \equiv 0(modp)$ ή $p \mid x_1$ (αφού $p > 2$) άρα $p \mid x_1^2$ δηλαδή $x_1^2 \equiv 0(modp)$, άτοπο, αφού $(\alpha, p) = 1$, δηλαδή $\alpha \not\equiv 0(modp)$. Θα αποδείξουμε ότι δεν υπάρχουν άλλες λύσεις $(modp)$.
Έστω x_2 μία άλλη λύση της ισοτιμίας. Τότε $x_1^2 \equiv x_2^2 \equiv \alpha(modp)$ οπότε $x_1^2 - x_2^2 \equiv 0(modp)$ ή $p \mid (x_1 - x_2)(x_1 + x_2)$.
Επομένως, αφού ο p είναι πρώτος, είτε $p \mid (x_1 - x_2)$, είτε $p \mid (x_1 + x_2)$.
Άρα: $x_2 \equiv x_1(modp)$ ή $x_2 \equiv -x_1(modp)$, δηλαδή, οποιαδήποτε λύση θα είναι ισότιμη με μία από τις $x_1, -x_1(modp)$.

Ορισμός
Αν η ισοτιμία $x^2 \equiv \alpha(modp)$, $(\alpha, p) = 1$ έχει λύση, τότε ο αριθμός α καλείται **τετραγωνικό κατάλοιπο** *modulo* p, διαφορετικά καλείται **μη-τετραγωνικό κατάλοιπο** *modulo* p.

Παράδειγμα
Να υπολογισθούν τα τετραγωνικά και μη-τετραγωνικά κατάλοιπα του αριθμού 11.
Λύση
Οι αριθμοί 1, 3, 4, 5, 9 είναι τετραγωνικά κατάλοιπα *mod* 11, αφού

$$\begin{aligned} 1^2 &\equiv 1(mod 11) \\ 2^2 &\equiv 4(mod 11) \\ 3^2 &\equiv 9(mod 11) \\ 4^2 &\equiv 5(mod 11) \\ 5^2 &\equiv 3(mod 11) \end{aligned}$$

ενώ οι αριθμοί 2, 6, 7, 8, 10 είναι μη-τετραγωνικά κατάλοιπα *mod* 11. Πράγματι, για τις τιμές αυτές του α δεν υπάρχουν ακέραιες τιμές του x ώστε $x^2 \equiv \alpha(mod 11)$,αφού αν

- $x \equiv 1$ ή $10(mod 11)$, τότε $x^2 \equiv 1(mod 11)$

- $x \equiv 2$ ή $9(mod 11)$, τότε $x^2 \equiv 4(mod 11)$
- $x \equiv 3$ ή $8(mod 11)$, τότε $x^2 \equiv 9(mod 11)$
- $x \equiv 4$ ή $7(mod 11)$, τότε $x^2 \equiv 5(mod 11)$
- $x \equiv 5$ ή $6(mod 11)$, τότε $x^2 \equiv 3(mod 11)$.

Γενικότερα για το πλήθος των τετραγωνικών καταλοίπων έχουμε το ακόλουθο θεώρημα:

Θεώρημα 3.1.2
Έστω p ένας πρώτος, $p > 2$. Στο σύνολο $\{1, 2, \ldots, p-1\}$ υπάρχουν ακριβώς $(p-1)/2$ τετραγωνικά κατάλοιπα και $(p-1)/2$ μη-τετραγωνικά κατάλοιπα *modulo* p.

Απόδειξη.
Χωρίζουμε το $\mathbf{Z}$ σε κλάσεις ισοτιμιών modp, και θεωρούμε τη συνάρτηση

$$f : \mathbf{Z} \longrightarrow \{1, 2, \ldots, p-1\}$$

η οποία απεικονίζει το x στο $y \equiv x^2(mod p)$, με $1 \leq y \leq p-1$. Είναι φανερό ότι στοιχεία της ίδιας κλάσης απεικονίζονται στο ίδιο στοιχείο. Ακόμη, σύμφωνα με το Θεώρημα 3.1.1, υπάρχουν ακριβώς δύο διαφορετικές τιμές του $x(mod p)$, άρα και δύο διαφορετικές κλάσεις για τις οποίες $f(x) = y$. Άρα το σύνολο τιμών της f θα περιέχει ακριβώς $\frac{p-1}{2}$ στοιχεία, τα οποία είναι εξ ορισμού όλα τα τετραγωνικά κατάλοιπα *modulo* p .

Ο Euler, το 1755, διατύπωσε το παρακάτω κριτήριο για τετραγωνικά κατάλοιπα *modulo* p:

Θεώρημα 3.1.3 (Κριτήριο Euler)
Ο ακέραιος $\alpha \neq 0$ είναι τετραγωνικό κατάλοιπο $mod p$, όπου p πρώτος, $p > 2$ και $(\alpha, p) = 1$ αν και μόνο αν

$$\alpha^{\frac{p-1}{2}} \equiv 1(mod p).$$

Απόδειξη.
Έστω ότι το $\alpha \neq 0$ είναι τετραγωνικό κατάλοιπο *modulo* p. Τότε θα υπάρχει ακέραιος x_0 τέτοιος ώστε $x_0^2 \equiv \alpha(mod p)$. Άρα έχουμε $x_0^{p-1} \equiv \alpha^{\frac{p-1}{2}}(mod p)$.

Από το θεώρημα του Fermat (βλέπε § 2.4) έχουμε $x_0^{p-1} \equiv 1(modp)$ οπότε $\alpha^{\frac{p-1}{2}} \equiv 1(modp)$.
Έστω ότι το α δεν είναι τετραγωνικό κατάλοιπο *modulo* p. Για όλους τους ακέραιους αριθμούς x, με $1 \leq x \leq p-1$ έχουμε $x^2 \not\equiv \alpha \pmod{p}$. Θεωρούμε τους αριθμούς

$$1x,\ 2x,\ 3x, \ldots, (p-1)x\ (modp).$$

Αυτοί οι αριθμοί είναι διαφορετικοί μεταξύ τους, αφού αν $\varkappa x \equiv \lambda x(modp)$ για κάποιους $\varkappa, \lambda$, τότε θα είχαμε $p \mid (\varkappa - \lambda)x$, οπότε $p \mid x$ ή $p \mid (\varkappa - \lambda)$. Άρα $p \mid \varkappa - \lambda$,αφού $1 \leq x \leq p-1$, δηλαδή $\varkappa \equiv \lambda(modp)$, οπότε $\varkappa$=λ, αφού $1 \leq \varkappa, \lambda \leq p-1$.
Έτσι οι αριθμοί αυτοί θα είναι οι αριθμοί $1, 2, 3, \ldots, p-1$ με διαφορετική διάταξη. Επειδή υποθέτουμε $1 \leq \alpha \leq p-1$, θα υπάρχει μοναδικό $y \in \{1, 2, 3, ..., p-1\}$ έτσι ώστε $xy \equiv \alpha(modp)$.
Επειδή $x^2 \not\equiv \alpha(modp)$ θα έχουμε $y \neq x$. Άρα μπορούμε να χωρίσουμε το σύνολο $\{1, 2, ..., p-1\}$ σε $\frac{p-1}{2}$ ζεύγη αριθμών ώστε το γινόμενο των αριθμών κάθε ζεύγους να είναι ισότιμο με $\alpha(modp)$.
Πολλαπλασιάζοντας τα ζεύγη μεταξύ τους προκύπτει ότι:

$$(p-1)! \equiv \alpha^{\frac{p-1}{2}}(modp).$$

Από το θεώρημα Wilson, $(p-1)! \equiv -1(modp)$, οπότε $\alpha^{\frac{p-1}{2}} \equiv -1(modp)$.
Έτσι αποδείξαμε ότι η παράσταση $\alpha^{(p-1)/2}$ παίρνει πάντα την τιμή $+1$ ή -1 και μάλιστα την πρώτη αν ο α είναι τετραγωνικό κατάλοιπο $(modp)$ και τη δεύτερη αν ο α δεν είναι τετραγωνικό κατάλοιπο $(modp)$.

Εφαρμογές 3.1

1. Να εξετάσετε αν οι παρακάτω αριθμοί είναι τετραγωνικά κατάλοιπα:
(i) Το 3 ως προς *modulo* 11.
(ii) Το 7 ως προς *modulo* 97.
(iii)Το 4 ως προς *modulo* 103.

Λύση.

(i)Χρησιμοποιώντας το κριτήριο Euler, έχουμε διαδοχικά :

$$\begin{aligned} 3^{\frac{11-1}{2}} = 3^5 &= 27 \cdot 9 \\ &\equiv 5 \cdot 9 \quad (mod 11) \\ &\equiv 45 \quad (mod 11) \\ &\equiv 1 \quad (mod 11) \end{aligned}$$

άρα ο 3 είναι τετραγωνικό κατάλοιπο *modulo* 11.
(ii) Όμοια,

$$\begin{aligned} 7^{\frac{97-1}{2}} = 7^{48} = 49^{24} &= 2401^{12} \\ &\equiv (-24)^{12} \quad (mod 97) \\ &\equiv 576^6 \quad (mod 97) \\ &\equiv (-6)^6 \quad (mod 97) \\ &\equiv (216)^2 \quad (mod 97) \\ &\equiv 22^2 \quad (mod 97) \\ &\equiv (-1) \quad (mod 97) \end{aligned}$$

άρα ο 7 είναι μη-τετραγωνικό κατάλοιπο *modulo* 97.
(iii)Ο 4 είναι τετραγωνικό κατάλοιπο *modulo* 103, αφού η $x = 2$ είναι λύση της ισοτιμίας $x^2 \equiv 4(mod 103)$.

Παρατήρηση

Το κριτήριο του Euler προσδιορίζει με απλό τρόπο αν ένας αριθμός α είναι τετραγωνικό κατάλοιπο $(mod p)$ (p πρώτος, $p > 2$, $(\alpha, p) = 1$), αλλά είναι αρκετά δύσχρηστο, αφού απαιτεί αρκετά μεγάλο πλήθος πράξεων της τάξης του $\log_2 p$ για μεγάλο p .

2. **Λήμμα του Gauss**
'Εστω p ένας πρώτος, $p > 2$ και α ακέραιος με $(\alpha, p) = 1$.
Θεωρούμε τους αριθμούς :

$$\alpha, 2\alpha, 3\alpha, \ldots, \frac{p-1}{2}\alpha \ (mod p).$$

'Εστω ν το πλήθος των αριθμών που είναι μεγαλύτεροι από $\frac{p}{2}$.
Να αποδειχθεί ότι ο α είναι τετραγωνικό κατάλοιπο $(mod p)$ αν και μόνο αν ο ν είναι άρτιος.

Απόδειξη.

Στην απόδειξη του Θεωρήματος 3.2.3 είδαμε ότι οι αριθμοί

$$\alpha, 2\alpha, 3\alpha, \ldots, \frac{p-1}{2}\alpha \ (mod p)$$

είναι όλοι διαφορετικοί μεταξύ τους.
'Εστω $\kappa_1, \kappa_2, ..., \kappa_\nu$ οι ν αριθμοί που είναι μεγαλύτεροι από το $\frac{p}{2}$ και $\lambda_1, \lambda_2, ..., \lambda_\mu$ οι $\mu = \frac{p-1}{2} - \nu$ υπόλοιποι αριθμοί που είναι μικρότεροι του $\frac{p}{2}$. (Επειδή p=περιττός δεν υπάρχει περίπτωση κάποιος αριθμός να είναι ίσος με $\frac{p}{2}$).
Αφού $\frac{p}{2} < \kappa_i < p$, θα έχουμε $0 < p - \kappa_i < \frac{p}{2}$, για κάθε i .
Θα αποδείξουμε ότι οι αριθμοί $p - \kappa_i$ είναι διαφορετικοί $(mod p)$ από τους $\lambda_1, \lambda_2, ..., \lambda_\mu$.
Πράγματι, αν είχαμε $p - \kappa_i \equiv \lambda_j \pmod{\text{p}}$ για κάποιους κ_i, λ_j τότε $\kappa_i + \lambda_j \equiv 0(mod p)$ ή $x\alpha + y\alpha \equiv 0(mod p)$, όπου $\kappa_i = x\alpha, \lambda_j = y\alpha$, άρα $p \mid (x + y)$, αφού (α, p)=1.
Αυτό όμως είναι αδύνατο, αφού $2 \leq x + y \leq p - 1$. Επιπλέον από την αρχική παρατήρηση οι $p - \kappa_1, p - \kappa_2, \ldots, p - \kappa_\nu$ είναι επίσης διαφορετικοί μεταξύ τους.
Οπότε οι $\nu + \mu = \frac{p-1}{2}$ αριθμοί

$$p - \kappa_1, p - \kappa_2, \ldots, p - \kappa_\nu, \lambda_1, \lambda_2, \ldots, \lambda_\mu$$

είναι μία μετάθεση των αριθμών 1, 2, 3, ..., $\frac{p-1}{2}$.
'Ετσι

$$(p - \kappa_1)(p - \kappa_2) \cdots (p - \kappa_\nu)\lambda_1\lambda_2 \cdots \lambda_\mu \equiv \left(\frac{p-1}{2}\right)!(mod p) \ \ \text{ή}$$

$$(-1)^{\nu}\varkappa_1\varkappa_2\cdots\varkappa_\nu\lambda_1\lambda_2\cdots\lambda_\mu \equiv \left(\frac{p-1}{2}\right)!(modp).$$

Αλλά

$$\begin{aligned}\varkappa_1\varkappa_2\cdots\varkappa_\nu\lambda_1\lambda_2\cdots\lambda_\mu &= \alpha(2\alpha)(3\alpha)\cdots(\tfrac{p-1}{2}\alpha)\\ &= \left(\tfrac{p-1}{2}\right)!\alpha^{\frac{p-1}{2}},\end{aligned}$$

οπότε έχουμε :

$$\begin{aligned}(-1)^{\nu}\alpha^{\frac{p-1}{2}}\left(\tfrac{p-1}{2}\right)! &\equiv \left(\tfrac{p-1}{2}\right)!(modp) \quad \text{ή}\\ (-1)^{2\nu}\alpha^{\frac{p-1}{2}} &\equiv (-1)^{\nu}(modp) \quad \text{ή}\\ \alpha^{\frac{p-1}{2}} &\equiv (-1)^{\nu}(modp).\end{aligned}$$

Από το κριτήριο Euler, ο α είναι τετραγωνικό κατάλοιπο $(modp)$ αν και μόνο αν ο ν είναι άρτιος.

3. Να βρείτε τις λύσεις των εξισώσεων :
   (i) $x^2 \equiv 1(mod13)$
   (ii) $x^2 \equiv 3(mod13)$
   (iii) $x^2 \equiv 4(mod11)$
   (iv) $x^2 \equiv 3(mod11)$

   Λύση.

   (i) $x \equiv \pm 1(mod13)$ δηλαδή $x \equiv 1$ ή $12(mod13)$
   (ii) $x \equiv \pm 4(mod13)$ δηλαδή $x \equiv 4$ ή $9(mod13)$
   (iii) $x \equiv \pm 2(mod11)$ δηλαδή $x \equiv 2$ ή $9(mod11)$
   (iv) $x \equiv \pm 5(mod11)$ δηλαδή $x \equiv 5$ ή $6(mod11)$

Ασκήσεις 3.1

1. Βρείτε όλους τους ακεραίους x που ικανοποιούν την παρακάτω ισοτιμία $x^6 \equiv 1(mod 7)$.

2. Να βρείτε τα τετραγωνικά κατάλοιπα $mod 13$, $mod 19$, $mod 31$.

3. Για κάθε ακέραιο ν, να αποδειχθεί ότι ο ν^2+2 δεν είναι πολλαπλάσιο του 7.

3.2 Ο Συμβολισμός του Legendre

Ο Legendre παρατηρώντας ότι αν πολλαπλασιάσουμε δύο αριθμούς που είναι τετραγωνικά κατάλοιπα ή μη-τετραγωνικά κατάλοιπα προκύπτει ένα τετραγωνικό κατάλοιπο, ενώ το γινόμενο ενός τετραγωνικού καταλοίπου με ένα μη-τετραγωνικό κατάλοιπο δίνει μη-τετραγωνικό κατάλοιπο, προχώρησε στον παρακάτω συμβολισμό, που αποτελεί βασικό εργαλείο για τον προσδιορισμό τετραγωνικών καταλοίπων.

Ορισμός
Το σύμβολο του Legendre $\left(\frac{\alpha}{p}\right)$, όπου p πρώτος, $p > 2$ και $(\alpha, p) = 1$, ορίζεται ως εξής:

$$\left(\frac{\alpha}{p}\right) = \left\{ \begin{array}{ll} +1, & \text{αν το } \alpha \text{ είναι τετραγωνικό κατάλοιπο mod}p \\ -1, & \text{αν το } \alpha \text{ είναι μη-τετραγωνικό κατάλοιπο mod}p \end{array} \right\}$$

Χρησιμοποιώντας το κριτήριο του Euler μπορούμε να ορίσουμε ισοδύναμα το $\left(\frac{\alpha}{p}\right)$ ως εξής :

$$\left(\frac{\alpha}{p}\right) \equiv \alpha^{\frac{p-1}{2}} (mod p).$$

Ιδιότητες

$$\begin{array}{l} (\mathrm{i}) Αν\ \alpha \equiv \beta (mod p)\ τότε\ (\frac{\alpha}{p}) = (\frac{\beta}{p}) \\ (\mathrm{ii})(\frac{\alpha\beta}{p}) = (\frac{\alpha}{p})(\frac{\beta}{p}) \\ (\mathrm{iii})(\frac{\alpha^2}{p}) = 1 \\ (\mathrm{iv})(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} \\ (\mathrm{v})(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} \end{array}$$

Αποδείξεις
(i),(ii) Αποτελούν άμεση συνέπεια του κριτηρίου Euler και των ιδιοτήτων των ισοτιμιών.
(iii) Άμεση συνέπεια της (ii). Αλλιώς προκύπτει από τον ορισμό του τετραγωνικού καταλοίπου ότι η εξίσωση $x^2 \equiv \alpha^2 (mod p)$ έχει προφανή λύση την $x = \alpha$, οπότε το α είναι τετραγωνικό κατάλοιπο $(mod p)$.

(iv) Από το Κριτήριο Euler έχουμε ότι

$$\begin{aligned}(\tfrac{-1}{p}) &= (\tfrac{p-1}{p}) \equiv (p-1)^{\frac{p-1}{2}} \quad (mod p)\\ &\equiv (-1)^{\frac{p-1}{2}} \quad (mod p).\end{aligned}$$

Η ισοτιμία ισχύει ως ισότητα, αφού το δεξί μέλος παίρνει μόνο τις τιμές ± 1. Έτσι $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.

(v) Σύμφωνα με Λήμμα του Gauss, αρκεί να υπολογίσουμε πόσοι από τους αριθμούς $2, 4, 6, ..., p-1$ είναι μεγαλύτεροι του $\frac{p}{2}$.

Προσθέτοντας τους αριθμούς έχουμε :

$$\begin{aligned}2+4+6+\ldots+(p-1) &= \varkappa_1+\ldots+\varkappa_\nu+\lambda_1+\ldots+\lambda_\mu \quad \text{ή}\\ (p^2-1)/4 &= \varkappa_1+\ldots+\varkappa_\nu+\lambda_1+\ldots+\lambda_\mu \qquad (1)\end{aligned}$$

(Χρησιμοποιώντας τον ίδιο συμβολισμό με την απόδειξη του Λήμματος του Gauss).

Όμως είδαμε ότι οι αριθμοί

$$p-\varkappa_1, p-\varkappa_2, \ldots, p-\varkappa_\nu, \lambda_1, \lambda_2, \ldots, \lambda_\mu$$

είναι μια μετάθεση των $1, 2, \ldots, (p-1)/2$, οπότε

$$\begin{aligned}(p-\varkappa_1)+\ldots+(p-\varkappa_\nu)+\lambda_1+\ldots+\lambda_\mu &= 1+2+\ldots+\tfrac{p-1}{2} \quad \text{ή}\\ \nu p-(\varkappa_1+\ldots+\varkappa_\nu)+(\lambda_1+\ldots+\lambda_\mu) &= \tfrac{p^2-1}{8} \qquad (2)\end{aligned}$$

Από τις (1),(2) έχουμε $\nu p = \frac{p^2-1}{8}+2(\varkappa_1+\ldots+\varkappa_\nu)$ άρα $\nu p \equiv \frac{p^2-1}{8}(mod 2)$, οπότε $\nu \equiv \frac{p^2-1}{8}(mod 2)$, αφού ο p είναι περιττός.

Έτσι $(\frac{2}{p}) = (-1)^\nu = (-1)^{\frac{p^2-1}{8}}$.

Παρατήρηση

Οι ιδιότητες (iv), (v) μπορούν να γραφούν με την ακόλουθη "μνημονική" μορφή

$$\left(\frac{-1}{p}\right) = \left\{\begin{array}{ccc} 1 & , & \alpha\nu \quad p \equiv 1(mod 4)\\ -1 & , & \alpha\nu \quad p \equiv 3(mod 4)\end{array}\right\}$$

$$\left(\frac{2}{p}\right) = \left\{\begin{array}{ccc} 1 & , & \alpha\nu \quad p \equiv \pm 1(mod 8)\\ -1 & , & \alpha\nu \quad p \equiv \pm 3(mod 8)\end{array}\right\}$$

Οι προηγούμενες ιδιότητες μαζί με τον νόμο της τετραγωνικής αντιστροφής που περιγράφεται παρακάτω βοηθούν να υπολογίσουμε εύκολα οποιοδήποτε σύμβολο του Legendre και κατά συνέπεια να προσδιορίσουμε αν ένας ακέραιος είναι τετραγωνικό κατάλοιπο.

Θεώρημα 3.2.1 (Νόμος τετραγωνικής αντιστροφής του Legendre)
Αν οι p, q είναι δύο περιττοί πρώτοι τότε

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \left\{\begin{array}{r} +1, \text{αν τουλάχιστον ένας από} \\ \text{τους } p,\, q \equiv 1(mod 4) \\ \\ -1, \text{αν και οι δύο } p,\, q \equiv 3(mod 4) \end{array}\right\}.$$

Παρατήρηση
Επειδή τα σύμβολα του Legendre παίρνουν μόνο τις τιμές $+1$, -1 το να διαιρούμε με $\left(\frac{q}{p}\right)$ είναι το ίδιο με το να πολλαπλασιάζαμε με $\left(\frac{q}{p}\right)$. Συνεπώς ο νόμος της τετραγωνικής αντιστροφής γράφεται ισοδύναμα :

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right).$$

Εφαρμογές 3.2

1. Να υπολογισθούν τα σύμβολα του Legendre: $\left(\frac{26}{97}\right)$, $\left(\frac{93}{103}\right)$ και $\left(\frac{-24}{71}\right)$.

   Λύση.

   Χρησιμοποιώντας τις ιδιότητες των συμβόλων του Legendre έχουμε:

   (i)

$$\begin{aligned}\left(\frac{26}{97}\right) &= \left(\frac{2}{97}\right)\left(\frac{13}{97}\right)\\ &= (-1)^{\frac{97^2-1}{8}}\left(\frac{13}{97}\right)\\ &= \left(\frac{13}{97}\right)\\ &= (+1)\left(\frac{13}{97}\right)\\ &= \left(\frac{6}{13}\right)\\ &= \left(\frac{2}{13}\right)\left(\frac{3}{13}\right)\\ &= (-1)^{\frac{13^2-1}{8}}\left(\frac{3}{13}\right)\\ &= (-1)(+1)\left(\frac{13}{3}\right)\\ &= (-1)(+1)\left(\frac{1}{3}\right) = -1.\end{aligned}$$

(ii)

$$\begin{aligned}\left(\tfrac{93}{103}\right) &= \left(\tfrac{3}{103}\right)\left(\tfrac{31}{103}\right)\\ &= (-1)\left(\tfrac{103}{3}\right)\cdot(-1)\left(\tfrac{103}{31}\right)\\ &= \left(\tfrac{1}{3}\right)\cdot\left(\tfrac{10}{31}\right)\\ &= (+1)\left(\tfrac{2}{31}\right)\left(\tfrac{5}{31}\right)\\ &= (-1)^{\frac{31^2-1}{8}}\cdot(+1)\left(\tfrac{31}{5}\right)\\ &= (+1)(+1)\left(\tfrac{1}{5}\right) = +1.\end{aligned}$$

(iii)

$$\begin{aligned}\left(\tfrac{-24}{71}\right) &= \left(\tfrac{-1}{71}\right)\left(\tfrac{4}{71}\right)\left(\tfrac{2}{71}\right)\left(\tfrac{3}{71}\right)\\ &= (-1)^{\frac{71-1}{2}}(+1)\left(\tfrac{2}{71}\right)\left(\tfrac{3}{71}\right)\\ &= (-1)(+1)(-1)^{\frac{71^2-1}{8}}\cdot\left(\tfrac{3}{71}\right)\\ &= (-1)\cdot(-1)\left(\tfrac{71}{3}\right)\\ &= \left(\tfrac{2}{3}\right) = -1.\end{aligned}$$

2. Βρείτε την τιμή του συμβόλου Legendre $\left(\frac{3}{p}\right)$, όπου ο αριθμός $p > 3$ είναι πρώτος.

Λύση.

Εφαρμόζουμε το νόμο της τετραγωνικής αντιστροφής διακρίνοντας δύο περιπτώσεις:

Αν $p \equiv 1(mod4)$, τότε

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left\{ \begin{array}{lll} \left(\frac{2}{3}\right) = -1, & \alpha\nu & p \equiv 2(mod3) \\ \left(\frac{1}{3}\right) = 1, & \alpha\nu & p \equiv 1(mod3) \end{array} \right\}.$$

Αν $p \equiv 3(mod4)$, τότε

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = \left\{ \begin{array}{lll} -\left(\frac{2}{3}\right) = 1, & \alpha\nu & p \equiv 2(mod3) \\ -\left(\frac{1}{3}\right) = -1, & \alpha\nu & p \equiv 1(mod3) \end{array} \right\}.$$

Συνδυάζοντας τα παραπάνω έχουμε

$$\left(\frac{3}{p}\right) = \left\{ \begin{array}{rlllll} 1, & \alpha\nu & p \equiv 1 & \acute{\eta} & 11 & (mod12) \\ -1, & \alpha\nu & p \equiv 5 & \acute{\eta} & 7 & (mod12) \end{array} \right\}.$$

3. Να αποδειχθεί ότι ο αριθμός 3 δεν είναι τετραγωνικό κατάλοιπο $modp$, όπου ο $p > 3$ είναι πρώτος αριθμός της μορφής $4^x + 1$ ή $2^x - 1$ (αριθμοί Mersenne).

Απόδειξη.

Αν $p = 4^x + 1$, τότε $p \equiv 1(mod4)$ και $p \equiv 2(mod3)$, άρα

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Αν $p = 2^x - 1$, $(x \geq 3)$, τότε όπως είδαμε και στο 1ο Κεφάλαιο, ο αριθμός x είναι πρώτος.
Άρα έχουμε

$$p = 2^x - 1 \equiv (-1)^x - 1 \equiv -2 \equiv 1(mod3)$$

και

$$p = 2^x - 1 \equiv -1 \equiv 3(mod4).$$

Επομένως,

$$\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

Και στις δύο περιπτώσεις, ο αριθμός 3 δεν είναι τετραγωνικό κατάλοιπο $modp$.

4. Να βρείτε όλους τους πρώτους αριθμούς p για τους οποίους η ισοτιμία $x^2 \equiv 5(mod p)$ έχει λύση.

   Λύση.

   Για $p = 2$, η ισοτιμία $x^2 \equiv 5(mod 2)$ έχει λύση $x = 1$.
   Για $p = 3$, η ισοτιμία $x^2 \equiv 5(mod 3) \equiv 2(mod 3)$ δεν έχει λύση αφού μόνο ο αριθμός 1 είναι τετραγωνικό κατάλοιπο $mod 3$.
   Για $p = 5$, η ισοτιμία $x^2 \equiv 5(mod 5)$ έχει λύση $x = 0$.
   Για $p > 5$, έχουμε $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$. Τα τετραγωνικά κατάλοιπα $mod 5$ είναι οι αριθμοί 1,4, άρα η ισοτιμία $x^2 \equiv 5(mod p)$ έχει λύση αν και μόνο αν $p = 2$, $p = 5$ ή $p > 5$ με $p \equiv 1$ ή $4(mod 5)$.

5. Να αποδείξετε ότι η ισοτιμία $x^2 \equiv \varkappa(mod p)$ έχει ακριβώς $1 + \left(\frac{\varkappa}{p}\right)$ λύσεις, όπου ο p είναι ένας περιττός πρώτος και $\varkappa$ τέτοιος ώστε $(\varkappa, p) = 1$.

   Απόδειξη.

   Γνωρίζουμε ότι η ισοτιμία έχει λύση αν και μόνο αν το $\varkappa$ είναι τετραγωνικό κατάλοιπο $mod p$, και στην περίπτωση αυτή έχει ακριβώς δύο λύσεις. Αυτό συμβαίνει αν και μόνο αν $\left(\frac{\varkappa}{p}\right) = 1$, άρα το πλήθος των λύσεων είναι $1 + \left(\frac{\varkappa}{p}\right)$.

6. Χρησιμοποιώντας το κριτήριο Euler να εξετάσετε αν οι παρακάτω αριθμοί είναι τετραγωνικά κατάλοιπα:
   (i) Ο 2 ως προς $mod 5$
   (ii) Ο 4 ως προς $mod 7$
   (iii) Ο 3 ως προς $mod 13$

   Λύση.

   (i) $\left(\frac{2}{5}\right) \equiv 2^{\frac{5-1}{2}}(mod 5) \equiv 4(mod 5) \equiv -1$, άρα ο 2 δεν είναι τετραγωνικό κατάλοιπο $(mod 5)$.
   (ii) $\left(\frac{4}{7}\right) \equiv 4^{\frac{7-1}{2}}(mod 7) \equiv 64(mod 7) \equiv +1$, άρα ο 4 είναι τετραγωνικό κατάλοιπο $(mod 7)$.
   (iii) $\left(\frac{3}{13}\right) \equiv 3^{\frac{13-1}{2}}(mod 13) \equiv 729(mod 13) \equiv +1$, άρα ο 3 είναι τετραγωνικό κατάλοιπο $(mod 13)$.

7. Να εξετάσετε αν η ισοτιμία $x^2 \equiv 10(mod97)$ έχει λύση. Όμοια για την $x^2 \equiv 24(mod97)$. Για πόσες διαφορετικές τιμές του $\alpha(modulo97)$ έχει λύση η ισοτιμία $x^2 \equiv \alpha(mod97)$;

Λύση.

$\left(\frac{10}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{5}{97}\right) = (+1)\left(\frac{97}{5}\right) = \left(\frac{2}{5}\right) = -1$, άρα η ισοτιμία $x^2 \equiv 10(mod97)$ δεν έχει λύση.
Όμοια έχουμε $\left(\frac{24}{97}\right) = \left(\frac{4}{97}\right)\left(\frac{6}{97}\right) = (+1)\left(\frac{6}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{3}{97}\right) = (+1)\left(\frac{97}{3}\right) = (+1)(+1) = +1$, άρα η ισοτιμία $x^2 \equiv 24(mod97)$ έχει λύση.
Η ισοτιμία $x^2 \equiv \alpha(mod97)$ έχει λύση για $\frac{97-1}{2} = 48$ διαφορετικές τιμές του α.

8. Να εξετάσετε αν οι παρακάτω ισοτιμίες έχουν λύση
(i) $x^2 \equiv 17(mod29)$
(ii) $3x^2 \equiv 12(mod23)$
(iii) $x^2 + 4x \equiv 10(mod31)$

Λύση.

(i) $\left(\frac{17}{29}\right) = \left(\frac{29}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{4}{17}\right)\left(\frac{3}{17}\right) = (+1)\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1$, άρα η ισοτιμία δεν έχει λύση.
(ii) Ο αντίστροφος του 3 *modulo* 23 είναι ο 8. Πολλαπλασιάζοντας τη σχέση με 8 παίρνουμε : $x^2 \equiv 4(mod23)$ η οποία έχει προφανώς λύση αφού ο 4 ως τέλειο τετράγωνο είναι τετραγωνικό κατάλοιπο $(mod23)$.
(iii) Με συμπλήρωση τετραγώνου προκύπτει ότι : $(x+2)^2 \equiv 6(mod31)$, οπότε αρκεί να υπολογίσουμε το σύμβολο του Legendre $\left(\frac{6}{31}\right)$. Έχουμε $\left(\frac{6}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right) = (+1)(-1)\left(\frac{1}{3}\right) = -1$, άρα η ισοτιμία είναι αδύνατη.

Ασκήσεις 3.2

1. Έστω ένας πρώτος $p > 3$. Να αποδείξετε ότι η ισοτιμία $x^2 + 3 \equiv 0(modp)$ έχει λύση αν και μόνο αν $p = 6\kappa + 1$.

2. Έστω p ένας περιττός πρώτος και $\alpha_1, \alpha_2, \ldots, \alpha_\kappa$ τα τετραγωνικά του κατάλοιπα στο σύνολο $\Delta = \{1, 2, \ldots, p-1\}$. Να αποδείξετε ότι

$$A = \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_\kappa \equiv \left\{ \begin{array}{rcl} 1(modp), & \alpha\nu & p \equiv 3(mod4) \\ -1(modp), & \alpha\nu & p \equiv 1(mod4) \end{array} \right\}.$$

3. Έστω p και q δύο περιττοί πρώτοι τέτοιοι ώστε $p - q = 4\kappa$. Να αποδειχθεί ότι $\left(\frac{\kappa}{p}\right) = \left(\frac{\kappa}{q}\right)$.

3.3 Γενική μορφή λύσης ισοτιμίας δευτέρου βαθμού

Στις προηγούμενες παραγράφους μελετήσαμε την ισοτιμία $x^2 \equiv \alpha(mod p)$ όπου ο p ήταν πρώτος και εξετάσαμε πότε αυτή έχει λύση. Στην ενότητα αυτή θα μελετήσουμε τη γενική περίπτωση, όπου το p δεν είναι πρώτος.

Θεώρημα 3.3.1
Αν p πρώτος, $p \geq 3, r \geq 1$ και $(\alpha, p)=1$, τότε η ισοτιμία $x^2 \equiv \alpha(mod p^r)$ έχει λύση αν και μόνο αν $(\frac{\alpha}{p}) = 1$, δηλαδή αν και μόνο αν η $x^2 \equiv \alpha(mod p)$ είναι επιλύσιμη.

Απόδειξη.
Αν x_1 είναι λύση της $x^2 \equiv \alpha(mod p^r)$, τότε είναι λύση και της $x^2 \equiv \alpha(mod p)$, αφού:

$$x_1^2 \equiv \alpha(mod p^r) \text{ ή}$$

$$p^r \mid x_1^2 - \alpha \text{ ή}$$

$$p \mid x_1^2 - \alpha \text{ ή}$$

$$x_1^2 \equiv \alpha(mod p),$$

δηλαδή η $x^2 \equiv \alpha(mod p)$ είναι επιλύσιμη.
Αντίστροφα, θα αποδείξουμε με επαγωγή ότι και η $x^2 \equiv \alpha(mod p^r)$ έχει λύση. Υποθέτουμε ότι η $x^2 \equiv \alpha(mod p^{r-1})$ είναι επιλύσιμη και έχει λύση τη x_0.
Έστω $x = x_0 + p^{r-1}y$. Θεωρούμε την ισοτιμία

$$(x_0 + p^{r-1}y)^2 \equiv \alpha(mod p^r)$$

με άγνωστο τον y. Τότε

$$\begin{aligned} x_0^2 + p^{2r-2}y^2 + 2x_0yp^{r-1} &\equiv \alpha \pmod{p^r} \text{ ή} \\ x_0^2 + 2x_0yp^{r-1} &\equiv \alpha \pmod{p^r} \end{aligned}$$

αφού $p^r \mid p^{2r-2}$.
Επομένως, θα είναι $2x_0yp^{r-1} \equiv \alpha - x_0^2(mod p^r)$.
Αλλά $\alpha - x_0^2 \equiv 0(mod p^{r-1})$, άρα ο αριθμός $(\alpha - x_0^2)/p^{r-1}$ είναι ακέραιος, οπότε: $2x_0y \equiv (\alpha - x_0^2)/p^{r-1}(mod p)$.

Αυτή η εξίσωση είναι γραμμική και έχει λύση ως προς y, αφού $(x_0, p) = 1, p > 2$ και $(2x_0, p) = 1$.
Αν y_0 είναι μια λύση αυτής, τότε οι λύσεις της $x^2 \equiv \alpha(mod p^r)$ είναι

$$x = x_0 + p^{r-1}(y_0 + \varkappa p) = x_0 + p^{r-1}y_0 + \varkappa p^r, \varkappa \in \mathbf{Z},$$

άρα είναι επιλύσιμη.

Το ακόλουθο θεώρημα αποτελεί κριτήριο επίλυσης της τετραγωνικής ισοτιμίας ως προς modulo δύναμης του 2.

Θεώρημα 3.3.2
Η ισοτιμία $x^2 \equiv \alpha(mod 2^\varkappa), \varkappa \geq 3$, α περιττός, είναι επιλύσιμη αν και μόνο αν $\alpha \equiv 1(mod 8)$.

Απόδειξη.
Για $\varkappa$=3 η ισοτιμία γράφεται $x^2 \equiv \alpha(mod 8)$. Επειδή ο α είναι περιττός πρέπει και ο x να είναι περιττός. Όμως επειδή το τετράγωνο οποιουδήποτε περιττού είναι $1(mod 8)$, οπότε πρέπει $\alpha \equiv 1(mod 8)$. Αντίστροφα, αν $\alpha \equiv 1(mod 8)$, τότε η $x^2 \equiv 1(mod 8)$ έχει προφανείς λύσεις $x \equiv 1, 3, 5, 7(mod 8)$.
Έστω ότι η πρόταση ισχύει για κάποιο $\varkappa$ και έστω ότι η ισοτιμία $x^2 \equiv \alpha(mod 2^{k+1})$ είναι επιλύσιμη, με λύση x_0. Τότε $x_0^2 \equiv \alpha(mod 2^\varkappa)$, οπότε από την υπόθεση $\alpha \equiv 1(mod 8)$.
Αντίστροφα, αν $\alpha \equiv 1(mod 8)$ θέτουμε $x = x_0 + 2^k y$ και εργαζόμενοι όπως στο θεώρημα 3.4.1 διαπιστώνουμε ότι η ισοτιμία είναι επιλύσιμη.
Τέλος εύκολα παρατηρούμε ότι για τις ισοτιμίες $mod 2$, $mod 4$ ισχύουν τα παρακάτω:

- $x^2 \equiv 0(mod 2)$ έχει λύση $x \equiv 0(mod 2)$
- $x^2 \equiv 1(mod 2)$ έχει λύση $x \equiv 1(mod 2)$
- $x^2 \equiv 0(mod 4)$ έχει λύσεις $x \equiv 0, 2(mod 4)$
- $x^2 \equiv 1(mod 4)$ έχει λύσεις $x \equiv 1, 3(mod 4)$
- $x^2 \equiv 2(mod 4)$ δεν έχει λύση
- $x^2 \equiv 3(mod 4)$ δεν έχει λύση.

Το επόμενο θεώρημα ουσιαστικά ανάγει την ύπαρξη λύσης τετραγωνικών ισοτιμιών $x^2 \equiv \alpha(modm)$ στην εξέταση ύπαρξης λύσης των ισοτιμιών $x^2 \equiv \alpha(modp_i)$, όπου p_i είναι οι πρώτοι που διαιρούν τον m.

Θεώρημα 3.3.3
Έστω η ισοτιμία $x^2 \equiv \alpha(modm)$ όπου $m = m_1 \cdot \ldots \cdot m_k$ με $(m_i, m_j) = 1$, για κάθε i,j. Η παραπάνω ισοτιμία είναι επιλύσιμη αν και μόνο αν καθεμία από τις ισοτιμίες $x^2 \equiv \alpha(modm_i), i = 1, 2, \ldots, k$ είναι επιλύσιμη.

Απόδειξη.
Απλή.

Εφαρμογές 3.3

1. Να εξετάσετε αν η ισοτιμία $x^2 \equiv 12(mod 2989)$ έχει λύση.

   Λύση.

   Επειδή $2989 = 7^2 \cdot 61$, η ισοτιμία έχει λύση αν και μόνο αν $\left(\frac{12}{7}\right) = \left(\frac{12}{61}\right) = 1$. Όμως $\left(\frac{12}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{7}\right) = \left(\frac{2}{5}\right) = -1$, οπότε η ισοτιμία δεν έχει λύση.

Ασκήσεις 3.3

1. Να εξετάσετε αν οι παρακάτω ισοτιμίες έχουν λύση:
   (i) $x^2 \equiv 2(mod 61)$
   (ii) $x^2 \equiv -2(mod 61)$
   (iii) $x^2 \equiv 2(mod 118)$
   (iv) $x^2 \equiv -1(mod 365)$
   (v) $x^2 \equiv 73(mod 173)$
   (vi) $x^2 \equiv 42(mod 97)$

2. Να λυθούν οι ισοτιμίες:
   (i) $x^2 \equiv 1(mod 49)$
   (ii) $x^2 \equiv 2(mod 7^3)$
   (iii) $x^2 \equiv 9(mod 16)$
   (iv) $x^2 \equiv 4(mod 15)$

Γενικές Ασκήσεις 3ου Κεφαλαίου

1. Έστω ένας πρώτος αριθμός $p \geq 7$. Να αποδειχθεί ότι υπάρχουν δύο διαδοχικά τετραγωνικά κατάλοιπα *modp*.

2. Έστω ν, $\varkappa$ φυσικοί και p πρώτος τέτοιος ώστε

$$p > (\nu^2 + \nu + \varkappa)^2 + \varkappa.$$

Να αποδείξετε ότι ανάμεσα στους αριθμούς

$$\nu^2, \nu^2 + 1, \nu^2 + 2, \ldots, \nu^2 + \mu$$

όπου $\mu = (\nu^2 + \nu + \varkappa)^2 - \nu^2 + \varkappa$ υπάρχουν δύο x, y με $y - x = \varkappa$ τέτοιοι ώστε $\left(\frac{x}{p}\right) = \left(\frac{y}{p}\right) = 1$.

3. Να βρείτε όλα τα σύνολα θετικών ακεραίων ν με την ιδιότητα : "το σύνολο $\{\nu, \nu+1, \nu+2, \nu+3, \nu+4, \nu+5\}$ μπορεί να διαμερισθεί σε δύο σύνολα, έτσι ώστε το γινόμενο των αριθμών του ενός συνόλου να είναι ίσο με το γινόμενο των αριθμών του άλλου".
(12η ΔΜΟ,1970 Ουγγαρία)

Επαναληπτικές Ερωτήσεις Πολλαπλής Επιλογής

Να αιτιολογήσετε την απάντησή σας στις ακόλουθες ερωτήσεις:

1. Ο αριθμός $2^{10}-1$ διαιρείται ακριβώς με τον αριθμό:
   (α) 2 (β) 10 (γ) 3 (δ) 4 (ε) 8

2. Ο αριθμός 2^7-2 διαιρείται ακριβώς με τον 7 και ο 2^5-2 διαιρείται ακριβώς με τον 5. Το άθροισμα των δύο πηλίκων είναι:
   (α) 0 (β) 23 (γ) 24 (δ) $48\cdot\frac{24}{25}$ (ε) $24\cdot\frac{24}{35}$

3. Ένας φυσικός αριθμός ο οποίος είναι πολλαπλάσιο του 15, αλλά όχι πολλαπλάσιο του 18, είναι:
   (α) 180 (β) 320 (γ) 360 (δ) 420 (ε) 540

4. Έστω ο αριθμός $N=1\cdot 2\cdot 3\cdot 4\cdot ...\cdot 18\cdot 19\cdot 20=20!$. Από τους παρακάτω αριθμούς ποιος είναι ο μεγαλύτερος διαιρέτης του N;
   (α) 9.000.000 (β) 900.000 (γ)90.000 (δ) 9.000 (ε) 900

5. Η μικρότερη τιμή του φυσικού ν ώστε ο 60κ να είναι τέλειο τετράγωνο ακεραίου, είναι:
   (α) 60 (β) 15 (γ) 6 (δ) 45 (ε) 9

6. Τέλειος αριθμός καλείται ένας φυσικός όταν ισούται με το άθροισμα των γνήσιων διαιρετών του. Για παράδειγμα έχουμε ότι ο αριθμός 6=1+2+3 είναι τέλειος. Ο επόμενος τέλειος αριθμός είναι:
   (α) 28 (β) 16 (γ) 24 (δ) 8 (ε) 36

7. Ο ελάχιστος φυσικός που αφήνει υπόλοιπα 1, 4, 1, όταν διαιρεθεί με τους 3, 5, 11 αντίστοιχα βρίσκεται μεταξύ των αριθμών:
   (α) 11 και 20 (β) 21 και 30 (γ) 31 και 40 (δ) 41 και 50 (ε) 61 και 70

8. Αν ν είναι ένας τυχαίος φυσικός, τότε ένα σίγουρο πολλαπλάσιο του 3 είναι ο αριθμός:
   (α) (ν+1)(ν+4) (β) ν(ν+2)(ν+4) (γ) ν(ν+2)(ν+6) (δ) ν(ν+3)(ν-3)
   (ε) (ν+2)(ν+3)(ν+5)

9. Το λεωφορείο Βούλα-Πειραιά φεύγει από την αφετηρία της Βούλας κάθε 12 λεπτά, ενώ το λεωφορείο Βούλα-Αθήνα φεύγει κάθε 20

λεπτά. Αν τα δύο λεωφορεία φεύγουν από την αφετηρία της Βούλας στις 1.00 μμ ταυτόχρονα, μια άλλη ώρα που θα αναχωρήσουν μαζί είναι:
(α) 1:32 μμ (β) 2:20 μμ (γ) 2:40μμ (δ) 3:00 μμ (ε) 3:40 μμ

10. Ένας πιθανός έβδομος όρος της ακολουθίας $1, 2, 5, 10, 17, \ldots$ είναι:
(α) 24 (β) 26 (γ) 37 (δ) 50 (ε) κανείς από αυτούς

11. Το άθροισμα $200 - 199 + 198 - 197 + \ldots - 3 + 2 - 1$ είναι:
(α) 99 (β) 200 (γ) 100 (δ) 101 (ε) 1

12. Το άθροισμα των πρώτων ν όρων μιας ακολουθίας δίνεται από τον τύπο $\Sigma = \nu(\nu + 1)(\nu + 2)$. Ο δέκατος όρος της ακολουθίας είναι:
(α) 114 (β) 330 (γ) 396 (δ) 600 (ε) 1320

13. Ο μικρότερος φυσικός ν, για τον οποίον το άθροισμα $\nu + 2\nu + 3\nu + \ldots + 100\nu$, είναι τέλειο τετράγωνο ακεραίου, είναι ο αριθμός:
(α) 100 (β)101 (γ) 202 (δ) 5050 (ε) κανείς από αυτούς

14. Αν μ και ν είναι δύο φυσικοί αριθμοί τέτοιοι ώστε $\mu^2 - \nu^2 = 29$, τότε το γινόμενο μν βρίσκεται μεταξύ των αριθμών:
(α) 0 και 100 (β) 100 και 150 (γ) 150 και 200 (δ) 201 και 250 (ε) 250 και άνω.

15. Ένας μαθητής διαιρεί δύο αριθμούς και βρίσκει το αποτέλεσμα $4,4285714$. Ποια διαίρεση από αυτές που ακολουθούν μπορεί να έκανε ο μαθητής;
(α) 63 : 14 (β) 31 : 7 (γ) 44285 :10 (δ) 40 : 9 (ε) 199 : 45
(Παρατήρηση: Να μην χρησιμοποιηθεί υπολογιστής τσέπης).

16. Το πλήθος των πρώτων αριθμών που είναι μικρότεροι του 10000 και το άθροισμα των ψηφίων τους είναι 2 ή 3, είναι:
(α) 4 (β) 3 (γ) 6 (δ) 5 (ε) 2

Επαναληπτικές Προτεινόμενες Ασκήσεις

1. Βρείτε το άθροισμα των διαιρετών του 24.

2. Βρείτε το σύνολο όλων των πρώτων αριθμών μεταξύ του 6 και του 50.

3. Βρείτε το ελάχιστο φυσικό ν, έτσι ώστε ο 120ν να είναι τέλειο τετράγωνο ακεραίου.

4. Βρείτε το ελάχιστο φυσικό ν, έτσι ώστε ο 12ν να είναι πολλαπλάσιο του 56.

5. Γνωρίζοντας ότι $12345679 \cdot 9 = 111111111$ βρείτε έναν φυσικό ν, τέτοιον ώστε $12345679 \cdot \nu = 666666666$.

6. Η ηλικία του Γιώργου αν διαιρεθεί με τους αριθμούς 2, 3, 4, 5 ή 6 αφήνει πάντα υπόλοιπο 1. Να υπολογισθεί η μικρότερη δυνατή ηλικία του Γιώργου αν γνωρίζουμε ότι είναι μεγαλύτερος των 2 ετών.

7. Το κουδούνι του σχολείου χτυπά κάθε 42 λεπτά, ενώ μια σειρήνα από το διπλανό εργοτάξιο ηχεί κάθε 36 λεπτά. Αν ακούστηκαν μαζί στις 9:00 πμ, πότε θα ξαναηχήσουν ταυτόχρονα;

8. Χρησιμοποιώντας από μια φορά τα ψηφία 1, 2, 3, 4 και 5 να σχηματίσετε έναν πενταψήφιο αριθμό αβγδε, τέτοιον ώστε να διαιρούνται ακριβώς με τους αριθμούς 4, 5 και 3, αντίστοιχα.

9. Βρείτε το άθροισμα των 25 πρώτων όρων της ακολουθίας

$$1, 2, -3, 4, 5, -6, 7, 8, -9, 10, \ldots$$

10. Βρείτε το άθροισμα των ψηφίων όλων των όρων της ακολουθίας $1, 2, 3, \ldots, 99, 100$.

11. Βρείτε το μικρότερο τέλειο τετράγωνο ακεραίου που έχει τρεις διαφορετικούς πρώτους παράγοντες.

12. Αν x και y είναι δύο φυσικοί αριθμοί τέτοιοι ώστε $13x+8y = 1992$, να υπολογισθεί η ελάχιστη δυνατή τιμή του αθροίσματος $x + y$.

13. Βρείτε όλους του φυσικούς μεταξύ του 100 και του 1000 με άθροισμα ψηφίων ίσο με 10.

14. Βρείτε 4 διαδοχικούς φυσικούς τέτοιους ώστε ο μικρότερος να είναι πολλαπλάσιο του 5, ο δεύτερος πολλαπλάσιο του 7, ο τρίτος πολλαπλάσιο του 9 και ο μεγαλύτερος να είναι πολλαπλάσιο του 11.

15. Να αποδειχθεί ότι ο αριθμός $E = (3+2\sqrt{2})^{2\nu-1} + (3-2\sqrt{2})^{2\nu-1}$ είναι τέλειο τετράγωνο ακεραίου, για κάθε φυσικό ν.

16. Σε ένα μαγαζί πωλούνται κρουασάν σε πακέτα των 7, 13 ή 25 τεμαχίων. Δηλαδή για να αγοράσουμε 14 κρουασάν πρέπει να αγοράσουμε 2 πακέτα των 7 τεμαχίων, ενώ δεν μπορούμε να αγοράσουμε 15 ακριβώς κρουασάν. Να υπολογισθεί το μέγιστο πλήθος κρουασάν που δεν μπορούμε να παραγγείλουμε με συνδυασμό αυτών των πακέτων.

Κεφάλαιο 4

Η εξέλιξη της Θεωρίας των Αριθμών

4.1 Εισαγωγή

Η Θεωρία Αριθμών αποτελεί ίσως των μοναδικό κλάδο των Μαθηματικών, του οποίου η δομή στηρίζεται περισσότερο στα άλυτα προβλήματα, παρά στα ήδη λυμένα. Τα σημαντικά άλυτα προβλήματα που υπάρχουν στη Θεωρία Αριθμών είναι πολλές φορές "προβλήματα-ντόμινο", που αν λυθούν θα οδηγήσουν στην επίλυση και πολλών άλλων.

Είναι λοιπόν, αναγκαία η γνώση της εξέλιξης της Θεωρίας Αριθμών και του σημείου στο οποίο έχουν φθάσει οι προσεγγίσεις των ερευνητικών προβλημάτων της.

Ας επισημάνουμε αρχικά δύο σημαντικές διαπιστώσεις που παρατηρούνται συχνά στη Θεωρία Αριθμών. Η πρώτη αφορά στο ότι παρατηρήσεις που ισχύουν για μικρούς φυσικούς ν, τις περισσότερες φορές δεν επεκτείνονται για μεγάλους–αυτό είναι γνωστό ως ο **"Νόμος των μικρών αριθμών"**. Ένα χαρακτηριστικό παράδειγμα αποτελούν οι αριθμοί Cullen : $\nu \cdot 2^{\nu} + 1$. Οι αριθμοί αυτοί είναι σύνθετοι για κάθε φυσικό ν, με $2 \leq \nu \leq 1000$ εκτός από τον 141. Η δεύτερη διαπίστωση είναι ότι συχνά οδηγούμαστε σε **μη αναμενόμενα αποτελέσματα** όπως φαίνεται στο ακόλουθο παράδειγμα, το οποίο προέρχεται από ένα πρόβλημα της Μαθηματικής Ολυμπιάδας της Μόσχας:
"Να βρεθούν όλες οι τριάδες φυσικών, διάφορων του 1, έτσι ώστε αν

στο γινόμενο οποιωνδήποτε δύο από αυτούς, προσθέσουμε τη μονάδα, να προκύψει αριθμός που διαιρείται από τον τρίτο αριθμό της τριάδας". Η απάντηση είναι 2, 3, 7 και μία πιθανή λύση δίνεται παρακάτω.

Ας θεωρήσουμε (x, y, z) μία λύση με $2 \leq x < y < z$. Τότε έχουμε ότι

$$\begin{aligned} x \mid yz+1 \quad &\text{ή} \quad yz+1 = k_1 x \\ y \mid zx+1 \quad &\text{ή} \quad zx+1 = k_2 y \\ z \mid xy+1 \quad &\text{ή} \quad xy+1 = k_3 z \end{aligned}$$

όπου $k_1, k_2, k_3 \in \mathbf{N}$. Πολλαπλασιάζοντας κατά μέλη τις τρεις ισότητες έχουμε ότι :

$$xyz(xyz+x+y+z) + yz + zx + xy + 1 = k_1 k_2 k_3 xyz.$$

Επομένως $xyz \mid yz + zx + xy + 1$, οπότε

$$yz + zx + xy + 1 = Axyz \quad \text{ή} \quad \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{xyz} = A,$$

όπου $A \in \mathbf{N}$. Η μέγιστη τιμή του A επιτυγχάνεται για τις ελάχιστες τιμές των x, y, z, δηλαδή $x = 2$, $y = 3$ και $z = 4$ (ουσιαστικά $z \geq 5$). Τότε έχουμε ότι

$$A \leq \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{2 \cdot 3 \cdot 4} = \frac{27}{24},$$

όμως $A \in \mathbf{N}$, οπότε $A = 1$. Συνεπώς, αρκεί να βρούμε όλες τις τριάδες φυσικών x, y, z που ικανοποιούν τις ανισότητες $2 \leq x < y < z$ και την ισότητα:

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{xyz} = 1.$$

Αρχικά θα αποδείξουμε ότι $x = 2$.

Πράγματι, αν ήταν $x \geq 3$, τότε $y \geq 4$, $z \geq 5$ και

$$1 = \frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{x \cdot y \cdot z} \leq \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{3 \cdot 4 \cdot 5} = \frac{4}{5}, \text{ άτοπο.}$$

Καταλήγουμε λοιπόν ότι τα y, z ικανοποιούν την εξίσωση

$$1 = \frac{1}{2} + \frac{1}{y} + \frac{1}{z} + \frac{1}{2 \cdot y \cdot z} \quad \text{ή} \quad \frac{5}{z-2} = y - 2,$$

οπότε $(z-2) \mid 5$ και είτε $z=3$, είτε $z=7$ που συνεπάγεται ότι $y=7$ ή $y=3$ αντιστοιχα. Επομένως η τριάδα (2, 3, 7) είναι η μοναδική που ικανοποιεί το ζητούμενο.

Όμοια αποδεικνύεται ότι η μοναδική τετράδα φυσικών με την ιδιότητα το γινόμενο οποιωνδήποτε τριών από αυτούς αυξανόμενο κατά 1, να διαιρείται από τον τέταρτο είναι η $(2, 3, 7, 43)$.

Θα φαινόταν πολύ φυσιολογικό να γενικεύσουμε τα προηγούμενα αποτελέσματα ως εξής:
"Έστω ν φυσικοί αριθμοί, $\alpha_1, \alpha_2, \ldots, \alpha_\nu$, διάφοροι του 1, τέτοιοι ώστε το γινόμενο οποιωνδήποτε $(\nu-1)$ από αυτούς αυξανόμενο κατά 1, να διαιρείται από τον αριθμό που απομένει από τους ν δοσμένους. Αν στο σύνολο των ν αριθμών $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ προσθέσουμε και τον αριθμό $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_\nu + 1$ τότε το νέο σύνολο των $(\nu+1)$ αριθμών, έχει την ιδιότητα ότι το γινόμενο οποιωνδήποτε ν αριθμών από αυτούς αυξανόμενο κατά 1, διαιρείται από τον αριθμό που απομένει.
Όμως η πρόταση αυτή δεν ισχύει! Για $\nu = 5$ εκτός από τη λύση $(2, 3, 7, 43, 1807)$ έχουμε και τη λύση $(2, 3, 7, 47, 365)$. Το πρόβλημα της μοναδικότητας των λύσεων παραμένει ακόμη ανοιχτό.

Στη συνέχεια θα περιγράψουμε τη μαθηματική εξέλιξη της Θεωρίας των Αριθμών σε μερικούς σημαντικούς τομείς της, οι περισσότεροι από τους οποίους δημιουργήθηκαν από την επιμονή των μαθηματικών να αντιμετωπίσουν τα ανοιχτά προβλήματα της Θεωρίας Αριθμών.

4.2 Η κατανομή των πρώτων

Θα ξεκινήσουμε τη μελέτη μας με την κατανομή των πρώτων αριθμών μέσα στο σύνολο των φυσικών, καθώς θεωρήθηκε από το σύνολο των ερευνητών το βασικότερο ερώτημα που θα οδηγούσε στη θεμελίωση της Θεωρίας των Αριθμών. Είναι γνωστή σε όλους μας η απόδειξη του Ευκλείδη της ύπαρξης άπειρων πρώτων αριθμών (βλ. Θεώρ.1.6.4). Μόλις όμως πριν από εκατό περίπου χρόνια αποδείχθηκε το παρεμφερές θεώρημα των πρώτων αριθμών το οποίο σχετίζεται με το πώς αυξάνεται το πλήθος των πρώτων αριθμών που υπάρχουν σε ένα διάστημα σε σχέση με το πλάτος του διαστήματος αυτού.

οπότε $(z-2) \mid 5$ και είτε $z=3$, είτε $z=7$ που συνεπάγεται ότι $y=7$ ή $y=3$ αντιστοιχα. Επομένως η τριάδα (2, 3, 7) είναι η μοναδική που ικανοποιεί το ζητούμενο.

Όμοια αποδεικνύεται ότι η μοναδική τετράδα φυσικών με την ιδιότητα το γινόμενο οποιωνδήποτε τριών από αυτούς αυξανόμενο κατά 1, να διαιρείται από τον τέταρτο είναι η $(2, 3, 7, 43)$.

Θα φαινόταν πολύ φυσιολογικό να γενικεύσουμε τα προηγούμενα αποτελέσματα ως εξής:
"Έστω ν φυσικοί αριθμοί, $\alpha_1, \alpha_2, \ldots, \alpha_\nu$, διάφοροι του 1, τέτοιοι ώστε το γινόμενο οποιωνδήποτε $(\nu-1)$ από αυτούς αυξανόμενο κατά 1, να διαιρείται από τον αριθμό που απομένει από τους ν δοσμένους. Αν στο σύνολο των ν αριθμών $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ προσθέσουμε και τον αριθμό $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_\nu + 1$ τότε το νέο σύνολο των $(\nu+1)$ αριθμών, έχει την ιδιότητα ότι το γινόμενο οποιωνδήποτε ν αριθμών από αυτούς αυξανόμενο κατά 1, διαιρείται από τον αριθμό που απομένει.
Όμως η πρόταση αυτή δεν ισχύει! Για $\nu = 5$ εκτός από τη λύση $(2, 3, 7, 43, 1807)$ έχουμε και τη λύση $(2, 3, 7, 47, 365)$. Το πρόβλημα της μοναδικότητας των λύσεων παραμένει ακόμη ανοιχτό.

Στη συνέχεια θα περιγράψουμε τη μαθηματική εξέλιξη της Θεωρίας των Αριθμών σε μερικούς σημαντικούς τομείς της, οι περισσότεροι από τους οποίους δημιουργήθηκαν από την επιμονή των μαθηματικών να αντιμετωπίσουν τα ανοιχτά προβλήματα της Θεωρίας Αριθμών.

4.2 Η κατανομή των πρώτων

Θα ξεκινήσουμε τη μελέτη μας με την κατανομή των πρώτων αριθμών μέσα στο σύνολο των φυσικών, καθώς θεωρήθηκε από το σύνολο των ερευνητών το βασικότερο ερώτημα που θα οδηγούσε στη θεμελίωση της Θεωρίας των Αριθμών. Είναι γνωστή σε όλους μας η απόδειξη του Ευκλείδη της ύπαρξης άπειρων πρώτων αριθμών (βλ. Θεώρ.1.6.4). Μόλις όμως πριν από εκατό περίπου χρόνια αποδείχθηκε το παρεμφερές θεώρημα των πρώτων αριθμών το οποίο σχετίζεται με το πώς αυξάνεται το πλήθος των πρώτων αριθμών που υπάρχουν σε ένα διάστημα σε σχέση με το πλάτος του διαστήματος αυτού.

4.2.1 Το Θεώρημα των Πρώτων Αριθμών

Ας θεωρήσουμε ότι η συνάρτηση $\pi(x)$ εκφράζει το πλήθος των πρώτων αριθμών έως τον αριθμό x, τότε ο Ευκλείδης ουσιαστικά απέδειξε ότι $\pi(x) \to \infty$, όταν $x \to \infty$ και η απόδειξη αυτή οδηγεί στην ποσοτική εκτίμηση:

$$\pi(x) > \log(\log x).$$

Το θεώρημα των πρώτων αριθμών εκφράζει ότι:

$$\pi(x) \sim \frac{x}{\log x}, \text{ όταν } x \to \infty.$$

Η εικασία αυτή διατυπώθηκε αρχικά από τους Legendre και Gauss, πριν από 200 χρόνια περίπου και αποδείχθηκε ανεξάρτητα από τους Hadamard και de la Vallée Poussin το 1896. Η απόδειξή τους βασίσθηκε στη θεωρία μιγαδικών συναρτήσεων, την οποία ανέπτυξε ο Riemann στην περίφημη εργασία του το 1859, όπου παρουσίασε ότι τα μυστικά των πρώτων περικλείονται μέσα στη συνάρτηση ζήτα:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}.$$

Στην ταυτότητα αυτή, ως προς τη μιγαδική μεταβλητή $s = \sigma + it$, συνδέεται το άθροισμα όλων των φυσικών αριθμών με το γινόμενο μίας έκφρασης όλων των πρώτων αριθμών. Η σειρά αυτή και το γινόμενο συγκλίνουν όταν $\sigma > 1$.

Ουσιαστικά ο Euler ανακάλυψε την ταυτότητα, την οποία μελέτησε μόνο για πραγματικές μεταβλητές s. Ωστόσο, χρησιμοποιώντας ότι η σειρά $\prod_p(1 - 1/p^s)$ συγκλίνει στο μηδέν απέδειξε ότι η σειρά $\sum 1/p$ αποκλίνει, δίνοντας μία νέα απόδειξη στο θεώρημα του Ευκλείδη για το πλήθος των πρώτων αριθμών.

Ο Riemann απέδειξε ότι, ως μιγαδική συνάρτηση, η $\zeta(s)$ έχει αναλυτική επέκταση σε όλο το μιγαδικό s- επίπεδο, οπότε το μυστικό της κατανομής των πρώτων περικλείεται στα μιγαδικά σημεία μηδενισμού της $\zeta(s)$. Πράγματι, το θεώρημα των πρώτων αριθμών εκφράζει ότι η $\zeta(s)$ δεν μηδενίζεται στην κάθετη ευθεία $\sigma = 1$, ενώ η περίφημη "Εικασία του Riemann" εκφράζει ότι όλα τα σημεία μηδενισμού της $\zeta(s)$ ανήκουν στην ευθεία $\sigma = \frac{1}{2}$.

Αποδεικνύοντας ότι η $\zeta(s)$ δεν έχει σημεία μηδενισμού σε κάποια αριστερή περιοχή της ευθείας $\sigma = 1$, ο de la Vallée Poussin απέδειξε ότι το λογαριθμικό ολοκλήρωμα που πρότεινε ο Gauss αποτελεί καλύτερη προσέγγιση της συνάρτησης $\pi(x)$. Ειδικότερα, απέδειξε ότι, όταν $x \to \infty$, τότε:

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O\left(xe^{-c\sqrt{\log x}}\right),$$

όπου c είναι μία θετική σταθερά, και το σφάλμα της προσέγγισης είναι μικρότερο από $O\left(x/\log^\kappa x\right)$, για δοσμένο κ και μεγάλα x.

Πολλοί ερευνητές ασχολήθηκαν μέσα στον αιώνα αυτό, για να επεκτείνουν την περιοχή μη-μηδενισμού της $\zeta(s)$, με στόχο να αποδείξουν την Εικασία του Riemann, που ουσιαστικά εκφράζει ότι το σφάλμα προσέγγισης της $\pi(x)$ δεν είναι πολύ μεγαλύτερο της $\sqrt{x}$.

Οι αποδείξεις των Hadamard και de la Vallée Poussin απλοποιήθηκαν αργότερα από τον Landau. Ως το 1949 ήταν άγνωστο αν το θεώρημα των πρώτων αριθμών μπορούσε να λυθεί χρησιμοποιώντας στοιχειώδη θεωρήματα, δηλαδή θεωρήματα που μπορούν να αποδειχθούν χωρίς τη χρήση μιγαδικής ανάλυσης. Το 1949 οι Erdös και Selberg δημοσίευσαν μία τέτοια στοιχειώδη–αν και αρκετά μακροσκελή–απόδειξη.

4.2.2 Τα κενά ανάμεσα στους πρώτους

Μεγάλη ερευνητική προσπάθεια έχει καταβληθεί για τον προσδιορισμό των κενών ανάμεσα σε διαδοχικούς πρώτους. Το άνω φράγμα τέτοιων κενών προϋποθέτει την ύπαρξη ενός πρώτου p στο διάστημα $x < p \leq x + h$ και ο βασικός στόχος είναι το πλάτος του διαστήματος $h = h(x)$ να είναι σχετικά μικρό. Ενδεικτικό παράδειγμα είναι η Εικασία του Bertrand, ότι υπάρχει πάντα ένας πρώτος p σε κάθε διάστημα της μορφής $x < p \leq 2x$, όπου $x \geq 1$, δηλαδή σε κάθε διάστημα πλάτους $h = x$. Η πρόταση αυτή αποδείχθηκε αρχικά από τον Chebychev το 1848, ενώ το θεώρημα των πρώτων αριθμών δίνει το ισχυρότερο αποτελέσμα ότι: $h = \varepsilon x$, όπου ε οποιοσδήποτε μικρός θετικός αριθμός με την προϋπόθεση ότι ο x είναι αρκετά μεγάλος. Στατιστικές μελέτες έχουν οδηγήσει στην εικασία ότι $h = c(\log x)^2$, για κάποια σταθερά c, αλλά το φράγμα αυτό φαίνεται ιδιαίτερα δύσκολο να αποδειχθεί και μάλιστα θεωρείται από τα δυσκολότερα προβλήματα της Θεωρίας Αριθμών.
Το 1930 ο G. Hoheisal απέδειξε ότι υπάρχει $\theta < 1$ τέτοιο ώστε $h = x^\theta$,

και μάλιστα απέδειξε ότι μία αποδεκτή τιμή του θ είναι η

$$\theta = 1 - \frac{1}{33000}.$$

Για να προσδιορίσουμε λοιπόν το άνω φράγμα του προβλήματος, αρκεί να πετύχουμε μία εκτίμηση του μεγαλύτερου κάτω φράγματος θ_0 του συνόλου των αποδεκτών τιμών του θ. Μετά από πολλές βελτιώσεις, έχει αποδειχθεί ότι η καλύτερη εκτίμηση είναι λίγο κάτω από την $\theta_0 \leq 11/20$, ενώ αν δεχθούμε ως υπόθεση την εικασία του Riemann καταλήγουμε ότι $\theta_0 \leq 1/2$.
Για να αποδείξουμε όμως ότι $h = c(\log x)^2$ απαιτείται να αποδείξουμε ότι $\theta_0 = 0$! Το αποτελέσμα αυτό θα συνεπάγεται ότι για κάθε θετικό αριθμό ε (οσοδήποτε μικρό) και για αρκετά μεγάλο x θα υπάρχει ένας πρώτος αριθμός μεταξύ των x και $x + x^{\varepsilon}$.

Το ερώτημα που τέθηκε ήταν αν είναι δυνατόν τα κενά ανάμεσα στους πρώτους να είναι πολύ μικρά. Μία από τις περίφημες εικασίες ήταν αυτή των **"δίδυμων πρώτων"**, δηλαδή πρώτων p τέτοιων ώστε και οι $p + 2$ να είναι πρώτοι. Αν θέσουμε p_ν τον ν-οστό πρώτο και $g_\nu = p_{\nu+1} - p_\nu$, τότε η εικασία των δίδυμων πρώτων συνεπάγεται ότι $g_\nu = 2$ για άπειρες τιμές του ν. Η εικασία αυτή έχει επιβεβαιωθεί από πίνακες πρώτων και αριθμητικά δεδομένα, όπου φαίνεται ότι η g_ν έχει τιμές όλους τους άρτιους αριθμούς άπειρες φορές, αλλά κανείς δεν έχει αποδείξει ούτε τον ασθενέστερο ισχυρισμό ότι:

"Δεν ισχύει ότι $g_\nu \to \infty$ όταν $\nu \to \infty$."

Το θεώρημα των πρώτων αριθμών διατυπώνεται στη μορφή:

$$p_\nu \sim \nu \log \nu, \text{ όταν } \nu \to \infty,$$

οπότε μπορούμε να αποδείξουμε ότι η μέση τιμή της g_ν είναι η $\log \nu$, επομένως ισχύει ότι:

$$g_\nu < (1 + \varepsilon) \log \nu,$$

για άπειρες τιμές του ν.
Ο P. Erdös (1935) απέδειξε ότι υπάρχει $c < 1$, τέτοιος ώστε

$$g_\nu < c \log \nu,$$

για άπειρες τιμές του ν. Επίσης απέδειξε ότι η g_ν μπορεί να γίνεται αρκετά μεγαλύτερη της μέσης τιμής της $\log \nu$. Για να διατυπώσουμε ένα ακριβέστερο αποτέλεσμα της μελέτης του Erdős πρέπει να εισάγουμε τη συνάρτηση:

$$F(\nu) = \frac{(\log \nu)(\log(\log \nu))(\log(\log(\log(\log \nu))))}{(\log(\log(\log \nu)))^2}$$

Ο Erdős πρώτος απέδειξε ότι υπάρχει θετική σταθερά c τέτοια ώστε:

$$g_\nu > \frac{cF(\nu)}{\log(\log(\log(\log \nu)))}$$

για άπειρες τιμές του ν, και αργότερα ο R. A. Rankin το 1938 βελτίωσε την ανισότητα του Erdös ως εξής:

$$g_\nu > cF_\nu,$$

για κάθε θετική σταθερά $c < \frac{1}{3}$.
Το πρόβλημα των Erdös-Rankin–για την επίλυση του οποίου ο Erdős έδινε αμοιβή 10000 δολλάρια (ενώ ήταν πάμφτωχος)–ζητούσε να αποδειχθεί ότι η c είναι οποιαδήποτε αρκετά μεγάλη θετική σταθερά. Η σημερινή βέλτιστη εκτίμηση έχει γίνει από τους H. Maier και C. Pomerance το 1989, οι οποίοι απέδειξαν ότι η c είναι οποιαδήποτε σταθερά μέχρι την τιμή 1,31256 περίπου. Το γενικό πρόβλημα παραμένει ανοιχτό.

4.2.3 Πρώτοι σε αριθμητικές προόδους

Πολλά προβλήματα της προσθετικής ή πολλαπλασιαστικής Θεωρίας Αριθμών απαιτούν τη γνώση της κατανομής των πρώτων σε αριθμητική πρόοδο. Αν, λοιπόν, οι α και κ είναι πρώτοι μεταξύ τους, τότε η αριθμητική πρόοδος $\nu \equiv \alpha(mod \kappa)$ περιέχει άπειρους πρώτους. Το αποτελέσμα αυτό αποδείχθηκε το 1837 από τον Dirichlet σε μία πολύ σημαντική εργασία, η οποία δημιούργησε νέους ερευνητικούς ορίζοντες στην Ανάλυση και στην Άλγεβρα.

Μετά από την απόδειξη του θεωρήματος των πρώτων αριθμών δεν είναι δύσκολο να αποδείξουμε ότι για δοσμένη τιμή του κ, το πλήθος των πρώτων $p \leq x$ σε κάθε μία από τις παραπάνω αριθμητικές προόδους $\nu \equiv \alpha(mod \kappa)$ είναι ουσιαστικά το ίδιο. Για παράδειγμα, όλοι οι πρώτοι

για άπειρες τιμές του ν. Επίσης απέδειξε ότι η g_ν μπορεί να γίνεται αρκετά μεγαλύτερη της μέσης τιμής της $\log \nu$. Για να διατυπώσουμε ένα ακριβέστερο αποτέλεσμα της μελέτης του Erdős πρέπει να εισάγουμε τη συνάρτηση:

$$F(\nu) = \frac{(\log \nu)(\log(\log \nu))(\log(\log(\log(\log \nu))))}{(\log(\log(\log \nu)))^2}$$

Ο Erdős πρώτος απέδειξε ότι υπάρχει θετική σταθερά c τέτοια ώστε:

$$g_\nu > \frac{cF(\nu)}{\log(\log(\log(\log \nu)))}$$

για άπειρες τιμές του ν, και αργότερα ο R. A. Rankin το 1938 βελτίωσε την ανισότητα του Erdös ως εξής:

$$g_\nu > cF_\nu,$$

για κάθε θετική σταθερά $c < \frac{1}{3}$.
Το πρόβλημα των Erdös-Rankin–για την επίλυση του οποίου ο Erdős έδινε αμοιβή 10000 δολλάρια (ενώ ήταν πάμφτωχος)–ζητούσε να αποδειχθεί ότι η c είναι οποιαδήποτε αρκετά μεγάλη θετική σταθερά. Η σημερινή βέλτιστη εκτίμηση έχει γίνει από τους H. Maier και C. Pomerance το 1989, οι οποίοι απέδειξαν ότι η c είναι οποιαδήποτε σταθερά μέχρι την τιμή 1,31256 περίπου. Το γενικό πρόβλημα παραμένει ανοιχτό.

4.2.3 Πρώτοι σε αριθμητικές προόδους

Πολλά προβλήματα της προσθετικής ή πολλαπλασιαστικής Θεωρίας Αριθμών απαιτούν τη γνώση της κατανομής των πρώτων σε αριθμητική πρόοδο. Αν, λοιπόν, οι α και κ είναι πρώτοι μεταξύ τους, τότε η αριθμητική πρόοδος $\nu \equiv \alpha(mod \kappa)$ περιέχει άπειρους πρώτους. Το αποτελέσμα αυτό αποδείχθηκε το 1837 από τον Dirichlet σε μία πολύ σημαντική εργασία, η οποία δημιούργησε νέους ερευνητικούς ορίζοντες στην Ανάλυση και στην Άλγεβρα.

Μετά από την απόδειξη του θεωρήματος των πρώτων αριθμών δεν είναι δύσκολο να αποδείξουμε ότι για δοσμένη τιμή του κ, το πλήθος των πρώτων $p \leq x$ σε κάθε μία από τις παραπάνω αριθμητικές προόδους $\nu \equiv \alpha(mod \kappa)$ είναι ουσιαστικά το ίδιο. Για παράδειγμα, όλοι οι πρώτοι

$p > 5$ πρέπει να ανήκουν σε μία από τις τέσσερεις αριθμητικές προόδους $p \equiv \alpha(mod 10)$, όπου $\alpha = 1, 3, 7, 9$ και αναμένεται περίπου το ένα τέταρτο των πρώτων να έχει ως τελευταίο δεκαδικό ψηφίο το 3. Ωστόσο, πολλά προβλήματα οδηγούν σε αποτελέσματα όπου επιτρέπεται η μεταβολή του $mod x$ ως προς το x, δημιουργώντας μεγάλες δυσκολίες ως προς την ομοιομορφία του x.

Η Γενικευμένη Υπόθεση του Riemann εκφράζει ότι υπάρχει ομοιομορφία ως προς $mod x$, εφόσον $x \leq \sqrt{x}$, και για το λόγο αυτό πολλά προβλήματα της Θεωρίας Αριθμών επιλύονται με βάση τη συνθήκη αυτή. Το περίφημο θεώρημα των Siegel-Walfisz (1936) εκφράζει ότι για κάθε δοσμένο A, ισχύει το ομοιόμορφο φράγμα $x \leq \log^A x$.

Το 1974 απονεμήθηκε στον E. Bombieri το Fields Medal για την εργασία του πάνω σε ένα αξιοσημείωτο θεώρημα (1965) στο οποίο αποδεικνύεται ότι υπάρχει ένα είδος ομοιομορφίας ως προς το x, όταν παίρνει τιμές έως το $\sqrt{x}$. Από τότε το θεώρημα αυτό του Bombieri αντικατέστησε τη Γενικευμένη Υπόθεση του Riemann σε πάρα πολλές αποδείξεις αποτελεμάτων, σχετικών με πρώτους, τα οποία πλέον δεν έχουν συνθήκες.

4.3 Η μέθοδος των Hardy-Littlewood

Καμμία μέλετη της Θεωρίας Αριθμών δεν μπορεί να παραβλέψει τη μέθοδο των Hardy-Littlewood, η οποία είναι μία πολύ ισχυρή αναλυτική μέθοδος με πολλές εφαρμογές στην προσθετική Θεωρία Αριθμών. Θα την περιγράψουμε μέσα από την επιτυχή εφαρμογή της σε τρία περίφημα προβλήματα με τα οποία ωστόσο δεν ασχοληθήκαμε στα προηγούμενα κεφάλαια. Αυτά είναι

1. Η εκτίμηση της συνάρτησης διαμέρισης.
2. Οι εικασίες του Goldbach.
3. Το πρόβλημα του Waring.

4.3.1 Η συνάρτηση διαμέρισης p(ν).

Το πρώτο βασικό πρόβλημα της προσθετικής θεωρίας αριθμών είναι η μελέτη της συνάρτησης διαμέρισης $p(\nu)$, που η τιμή της ισούται με το

πλήθος των διαμερίσεων του φυσικού αριθμού ν. Ως διαμέριση του ν θεωρούμε την αναπαράστασή του ως άθροισμα φυσικών αριθμών, επιτρέποντας επαναλήψεις του ίδιου προσθετέου, χωρίς να παίζει ρόλο η διάταξη των προσθετέων. Για παράδειγμα έχουμε ότι $p(5) = 7$, αφού το 5 έχει τις εξής διαμερίσεις: 5, 4+1, 3+2, 3+1+1, 2+2+1, 2+1+1+1, 1+1+1+1+1.

Ο Euler συνειδητοποίησε ότι το κλειδί στη μελέτη της συνάρτησης διαμέρισης $p(\nu)$ είναι η χρήση δυναμοσειρών και απέδειξε ότι αν $p(0) = 1$, τότε:

$$F(x) \equiv \sum_{\nu=1}^{\infty} p(\nu)x^{\nu} = \prod_{m=1}^{\infty} \frac{1}{1-x^m}.$$

Η ιδέα ήταν ότι αποτελέσματα σχετικά με την $p(\nu)$ θα προκύπτουν από τη μέλετη της γεννήτριας συνάρτησης $F(x)$.

Ο Euler βρήκε επίσης τον "τύπο του πενταγώνου", ο οποίος εκφράζει την $p(\nu)$ ως άθροισμα διαφόρων τιμών $p(m)$ με $m < \nu$. Ωστόσο, ο τύπος αυτός μπορεί να εφαρμοσθεί μόνο για πολύ μικρές τιμές του ν (το p(100) υπολογίσθηκε μόλις στον αιώνα μας).
Είναι ιδιαίτερα ενδιαφέρον ότι ο Euler δεν προσπάθησε να εκτιμήσει την $p(\nu)$, παρ' όλο που θα ήταν εύκολο να οδηγηθεί στα φράγματα:

$$2^{\sqrt{\nu}} < p(\nu) < \nu^{3\sqrt{\nu}}, \quad \text{για } \nu > 1.$$

Στην περίφημη συνεργασία τους, στις αρχές του αιώνα, οι G. H. Hardy και S. Ramanujan, μελέτησαν σε βάθος τις εκτιμήσεις, ακόμα και τον υπολογισμό της $p(\nu)$, για μεγάλα ν. Με στοιχειώδεις μαθηματικές γνώσεις απέδειξαν ότι:

$$\log p(\nu) \sim \pi\sqrt{\frac{2\nu}{3}}, \quad \text{όταν } \nu \to \infty.$$

Ανακάλυψαν μία πρωτότυπη μέθοδο αντιμετώπισης του προβλήματος με αναλυτικές συναρτήσεις και χρησιμοποίησαν ασυμπτωτικές σειρές για να υπολογίσουν την $p(\nu)$. Αντικατέστησαν τη μεταβλητή x στη γεννήτρια συνάρτηση, με μιγαδική μεταβλητή z και θεώρησαν τη συνάρτηση $F(z)/z^{\nu+1}$, η οποία έχει πόλο $(\nu+1)$-οστής τάξης στο σημείο $z = 0$, γνωρίζοντας ότι το ολοκληρωτικό υπόλοιπο του πόλου αυτού είναι ακριβώς $p(\nu)$. Χρησιμοποιώντας το θεώρημα ολοκληρωτικών υπολοίπων του

Cauchy προκύπτει ότι:

$$p(\nu) = \frac{1}{2\pi i}\int_C \frac{F(z)}{z^{\nu+1}}dz,$$

όπου C είναι μία απλή, κλειστή καμπύλη που περιέχει το 0 και βρίσκεται μέσα στον μοναδιαίο κύκλο $|z| < 1$. Για να υπολογίσουν το ολοκλήρωμα αυτό, θεώρησαν το C ως κύκλο πολύ κοντά στον μοναδιαίο κύκλο τον οποίο χώρισαν σε τόξα που βρίσκονταν κοντά στις ανωμαλίες της $F(z)$, οι οποίες είναι οι ρίζες της μονάδας πετυχαίνοντας έτσι ένα ασυμπτωτικό ανάπτυγμα της $p(\nu)$.

Μία σειρά από διάσημες εργασίες των Hardy και Littlewood γύρω στο 1920, ανέπτυξαν τις προηγούμενες ιδέες στη μορφή μίας ισχυρής μεθόδου, επονομαζόμενη "η μέθοδος του κύκλου", με βάση την οποία το 1937 ο H. Rademacher τροποποίησε τον αρχικό ισχυρισμό των Hardy-Ramanujan και πέτυχε την έκφραση της $p(\nu)$ σε μορφή συγκλίνουσας σειράς, ως εξής:

$$p(\nu) = \frac{1}{\pi\sqrt{2}}\sum_{\varkappa=1}^{\infty} A_\varkappa(\nu)\sqrt{\varkappa}\frac{d}{d\nu}\left[\frac{\eta\mu h\left(\frac{\pi}{\varkappa}\sqrt{\frac{2}{3}\left(\nu-\frac{1}{24}\right)}\right)}{\sqrt{\nu-\frac{1}{24}}}\right]$$

όπου:

$$A_\varkappa(\nu) = \sum_{0<h\le\varkappa:(h,\varkappa)=1} \exp\left(\pi i s(h,\varkappa) - 2\frac{\pi i\nu h}{\varkappa}\right)$$

και

$$s(h,\varkappa) = \sum_{1\le r<\varkappa}\frac{r}{\varkappa}\psi\left(\frac{hr}{\varkappa}\right),$$

$$\psi(\lambda) = \lambda - [\lambda] - \frac{1}{2}.$$

Παρ' όλο που ο τύπος αυτός φαίνεται ιδιαίτερα πολύπλοκος, η χρήση του είναι σχετικά απλή. Για παράδειγμα, μία εικασία του Ramanujan εμφάνιζε ότι $6857 \mid p(3724)$. Εύκολα υπολογίζει κανείς ότι:

$$\begin{aligned} p(3724) = {} & 369088410501557041462324784149197 \\ & 5079872100078323221721160866875 = \\ = {} & 6875\cdot 536849607295375148542905951261058193 \\ & 3954182957428679580521 7. \end{aligned}$$

που αποδεικνύει την ορθότητα της εικασίας του Ramanujan. Ο ιδιοφυής αυτός τύπος της συνάρτησης $p(\nu)$ αποτελεί το σημαντικότερο αποτέλεσμα της "μεθόδου του κύκλου".

4.3.2 Το πρόβλημα του Goldbach

Το πρόβλημα του Goldbach είναι ένα ακόμα πρόβλημα που ταλαιπώρησε τους μαθηματικούς για αιώνες. Το 1742 ο Goldbach έστειλε στον Euler την περίφημη εικασία: "Κάθε άρτιος αριθμός μεγαλύτερος του 4 είναι άθροισμα δύο περιττών πρώτων".
Ο Goldbach παρατήρησε ότι τότε θα ισχύει και το αντίστοιχο δυϊκό πρόβλημα, δηλαδή ότι: "κάθε περιττός αριθμός μεγαλύτερος του 7 γράφεται ως άθροισμα τριών περιττών πρώτων".

Αριθμητικοί πειραματισμοί δείχνουν ότι οι εικασίες του Goldbach ισχύουν σχεδόν σίγουρα. Ωστόσο, ήταν ιδιαίτερα δύσκολο να αποδειχθούν καθώς αποτελούν προβλήματα της προσθετικής Θεωρίας Αριθμών που εμπλέκουν πρώτους. Έως την εμφάνιση της μεθόδου των Hardy-Littlewood, δεν υπήρχε κανένας τρόπος αντιμετώπισης του προβλήματος.

Το 1937 ο I. M. Vinogradov χρησιμοποιώντας τη μέθοδο του κύκλου, ολοκλήρωσε την απόδειξη της δεύτερης εικασίας του Goldbach αποδεικνύοντας ότι κάθε αρκετά μεγάλος περιττός φυσικός (μεγαλύτερος του 10^{43000}) γράφεται ως άθροισμα τριών περιττών πρώτων. Για τους υπόλοιπους φυσικούς μικρότερους του 10^{43000}, η απόδειξη ήταν πλέον εμπειρική. Ωστόσο, η μέθοδος των Hardy και Littlewood ήταν ανεπαρκής για την απόδειξη της 1ης εικασίας του Goldbach, καθώς αποδείχθηκε τελικά ότι "σχεδόν όλοι" οι άρτιοι αριθμοί γράφονται ως άθροισμα δύο πρώτων. Ένα άλλο σημαντικό αποτέλεσμα προέκυψε το 1973 από τον J.R. Chen που απέδειξε ότι κάθε μεγάλος άρτιος αριθμός γράφεται ως άθροισμα ενός πρώτου και ενός άλλου αριθμού, ο οποίος έχει το πολύ δύο πρώτους διαιρέτες. Ο Chen απέδειξε επιπλέον ότι υπάρχουν άπειροι πρώτοι p τέτοιοι ώστε ο $p+2$ είτε είναι πρώτος, είτε έχει μόνο δύο πρώτους διαιρέτες. Πρέπει επίσης να αναφέρουμε ότι το 1930, ο L. Schnirelmann δημιούργησε μία θεωρία πυκνότητας με την οποία κατέληξε στο συμπέρασμα ότι το σύνολο των φυσικών που γράφονται ως άθροισμα δύο πρώτων έχει θετική πυκνότητα Schnirelmann, οπότε κατέληξε ότι υπάρχει σταθερά c τέτοια ώστε κάθε φυσικός γράφεται ως άθροισμα το πολύ c πρώτων. Το πάνω φράγμα της σταθεράς c μέχρι σήμερα είναι 9.

4.3.3 Το πρόβλημα του Waring

Ακόμα και ο Διόφαντος (250 π.Χ.) γνώριζε ότι κάθε φυσικός γράφεται ως άθροισμα τεσσάρων τέλειων τετραγώνων, και φυσικά γνώριζε ότι υπήρχαν αριθμοί, όπως ο 7, για τον οποίο απαιτούνται ακριβώς τέσσερα τέλεια τετράγωνα. Κανείς ωστόσο δεν έθεσε το αντίστοιχο πρόβλημα για άθροισμα κύβων ή μεγαλύτερων δυνάμεων έως το 1770, όταν ο Waring, διετύπωσε τον "προκλητικό" ισχυρισμό ότι γνώριζε όλες τις απαντήσεις. Πιο συγκεκριμένα, ο Waring διετύπωσε ότι "κάθε φυσικός γράφεται ως άθροισμα 4 τετραγώνων, 9 κύβων, 19 τετάρτων δυνάμεων, κ.ο.κ." Ο ισχυρισμός αυτός έμεινε γνωστός ως το περίφημο πρόβλημα του Waring, το οποίο θα μπορούσε να είχε διατυπώσει ακριβέστερα ως εξής:
"Για κάθε $\kappa \geq 2$, υπάρχει $s = s(\kappa)$ έτσι ώστε κάθε φυσικός ν να γράφεται στη μορφή:

$$\nu = x_1^\kappa + x_2^\kappa + \ldots + x_s^\kappa, \;\; x_i \geq 0.$$

Επιπλέον, αν συμβολίσουμε με $g(\kappa)$ τον μικρότερο s τότε $g(2) = 4$, $g(3) = 9$ και $g(4) = 19$, ενώ υπάρχει μέθοδος εύρεσης του $g(\kappa)$, για κάθε κ."

Ο Lagrange απέδειξε ότι $g(2) = 4$, την ίδια χρονιά που ο Waring διετύπωσε την εικασία του. Το 1851 ο Jacobi ζήτησε από τον διάσημο αριθμομνήμονα Dase να τον βοηθήσει στον υπολογισμό πινάκων αναπαράστασης των αριθμών ως αθροίσματα κύβων και τετάρτων δυνάμεων. Ας επαναλάβουμε μερικά από τα πειράματά του με μικρούς αριθμούς. Για τα αθροίσματα κύβων θεωρούμε αρχικά $\nu < 27 = 3^3$. Αφού μπορούμε να χρησιμοποιήσουμε μόνο τους 2^3 και 1^3 για να αναπαραστήσουμε το ν, και $24 = 2^3 + 2^3 + 2^3$, προκύπτει ότι οι 24, 25 και 26 χρειάζονται 3, 4 και 5 κύβους αντίστοιχα. Όμως ο 23 χρειάζεται 9 κύβους. Για $\nu \geq 27$ ο Jacobi βρήκε ότι:

$$239 = 4^3 + 4^3 + 3^3 + 3^3 + 3^3 + 1^3 + 1^3 + 1^3 + 1^3$$

όπου απαιτούνται πάλι 9 κύβοι. Για $\nu > 239$ φαίνεται ότι 8 κύβοι είναι πάντα αρκετοί, ενώ φαίνεται ότι ο 454 είναι ο τελευταίος αριθμός γαι τον οποίο απαιτούνται 8 κύβοι, ενώ 7 κύβοι είναι αρκετοί για $\nu > 454$. Για αρκετό καιρό πίστευαν ότι για τον 8042 ήταν αναγκαίοι 8 κύβοι, αλλά τελικά βρέθηκε ότι:

$$8042 = 19^3 + 10^3 + 4^3 + 4^3 + 3^3 + 3^3 + 1^3.$$

Το 1893, ο Wilferich απέδειξε ότι κάθε φυσικός αριθμός γράφεται ως άθροισμα 9 κύβων, οπότε $g(3) = 9$. Στη συνέχεια, το 1909 ο E. Landau απέδειξε ότι κάθε μεγάλος αριθμός γράφεται ως άθροισμα 8 κύβων και το 1942 ο Y. V. Linnik απέδειξε ότι 7 κύβοι είναι αρκετοί. Αν συμβολίσουμε με $G(k)$ τον ελάχιστο αριθμό s για τον οποίο το πρόβλημα του Waring είναι επιλύσιμο για μεγάλους φυσικούς ν, τότε οι Landau και Linnik απέδειξαν ότι $G(3) \leq 8$ και $G(3) \leq 7$, αντίστοιχα.

Για τις τέταρτες δυνάμεις ας θεωρήσουμε αρχικά $\nu < 81 = 3^4$, οπότε μπορούμε να χρησιμοποιήσουμε μόνο το 2^4 και το 1^4, οπότε δεν είναι δύσκολο να εξακριβώσουμε ότι ο 79 χρειάζεται 19 τέταρτες δυνάμεις για να αναπαρασταθεί ως άθροισμά τους:

$$79 = 2^4 + 2^4 + 2^4 + 2^4 + 15 \cdot 1^4.$$

Ωστόσο, το αναμενόμενο αποτέλεσμα ότι $g(4) = 19$, αποδείχθηκε μόλις το 1989.

Δεν είναι ιδιαίτερα δύσκολη η γενίκευση της προηγούμενης μεθόδου ώστε να καταλήξουμε σε ένα κάτω φράγμα της $g(\kappa)$. Για δοσμένο κ, θεωρούμε τον αριθμό $\nu = q \cdot 2^\kappa - 1$, όπου ο q επιλέγεται όσο το δυνατόν μεγαλύτερος με βάση τον περιορισμό $\nu < 3^\kappa$.
Τότε έχουμε ότι:

$$q = \left[\left(\frac{3}{2}\right)^\kappa\right]$$

οπότε ο $\nu = (q-1)2^\kappa + (2^\kappa - 1) \cdot 1^\kappa$, γράφεται ως άθροισμα το λιγότερο $(2^\kappa + q - 2)$ κ-οστών δυνάμεων. Επομένως:

$$g(\kappa) \geq 2^\kappa + \left[\left(\frac{3}{2}\right)^\kappa\right] - 2$$

και η ισότητα ισχύει για όλα τα $\kappa \geq 2$.

Το 1909 ο D. Hilbert απέδειξε την ύπαρξη του s για κάθε κ, δηλαδή ότι $g(\kappa) < \infty$, αλλά ήταν πολύ δύσκολο να πετύχει ένα πάνω φράγμα του $g(\kappa)$ με τη μέθοδο που χρησιμοποίησε.

Οι Hardy και Littlewood με τη μέθοδο του κύκλου έδωσαν μία νέα απόδειξη του θεωρήματος του Hilbert. Εφαρμόζοντας μία βελτιωμένη μορφή της μεθόδου των Hardy και Littlewood, ο Vinogradov πέτυχε ένα άνω φράγμα για την $G(\kappa)$, το οποίο ήταν μικρότερο από την αναμενόμενη τιμή της $g(\kappa)$. Αυτό το αποτέλεσμα απετέλεσε τα θεμέλια αριθμητικών

υπολογισμών που οδήγησαν στην πλήρη σχεδόν απόδειξη της αρχικής εικασίας του Waring και η τιμή της $g(\kappa)$ είναι πλέον γνωστό ότι δίνεται από την αναμενόμενη τιμή για αρκετά μεγάλα κ. Επιπλέον, για κάθε δοσμένο κ, είναι εύκολο να εξακριβωθεί η μέθοδος εύρεσης του $g(\kappa)$ από την εικασία, με τη μελέτη του κλασματικού μέρους του $\left(\frac{3}{2}\right)^{\kappa}$. Συνδυάζοντας τα αποτελέσματα αρκετών μαθηματικών, γνωρίζουμε πλέον ότι αν ισχύει ότι

$$1-\left\{\left(\frac{3}{2}\right)^{\kappa}\right\} \geq \left(\frac{3}{4}\right)^{\kappa},$$

όπου $\{\theta\}$ είναι το κλασματικό μέρος του θ, τότε ισχύει ο αναμενόμενος τύπος για το $g(\kappa)$. Αφού το δεξί μέλος της ανισότητας φθίνει εκθετικά ως προς κ, δεν είναι περίεργο να βρεθεί αντιπαράδειγμα για την ανισότητα αυτή. Ο K. Mahler απέδειξε το 1957 ότι υπάρχει το πολύ πεπερασμένο πλήθος τέτοιων αντιπαραδειγμάτων ή ακόμα και κανένα. Δυστυχώς, για τεχνικούς λόγους, ο προσδιορισμός του $g(\kappa)$ για κάθε κ, δεν έχει ακόμη αναχθεί σε πεπερασμένου πλήθους αριθμητικούς υπολογισμούς. Η τιμή του $g(\kappa)$ εξαρτάται κυρίως από την αναπαράσταση μερικών μικρών φυσικών αριθμών, αλλά η μελέτη των περιπτώσεων $\kappa = 4, 5$ δεν είναι καθόλου τετριμμένη. Ο J. R. Chen το 1963 και οι R. Balasubramanian και J. M. Deshouillers το 1989 απέδειξαν αντίστοιχα τα αναμενόμενα αποτελέσματα $g(5) = 37$ και $g(4) = 19$. Η έρευνα σήμερα σχετικά με το πρόβλημα του Waring περιορίζεται στην εκτίμηση του $G(\kappa)$, μόνο για $\kappa = 2$ και 4.

4.4 Η Μέθοδος του Κόσκινου

Στο 1ο Κεφάλαιο παρουσιάσαμε το κριτήριο της ρίζας το οποίο μπορεί να χρησιμοποιηθεί ως μέθοδος διαχωρισμού των πρώτων $p \leq x$ από τους σύνθετους, η οποία είναι γνωστή και ως **κόσκινο του Ερατοσθένη.** Η ιδέα είναι ότι η διαγραφή από μία λίστα με όλους τους αριθμούς έως τον x, των πολλαπλασίων όλων των πρώτων $p \leq \sqrt{x}$, οπότε οι εναπομείναντες αριθμοί θα είναι όλοι πρώτοι. Πολλές επεκτάσεις αυτής της μεθόδου είναι γνωστές και σε αυτή την ενότητα παρουσιάζουμε μερικές.

Ο Legendre το 1790 εφάρμοσε την αρχή Εγκλεισμού-Αποκλεισμού της Συνδυαστικής και οδηγήθηκε στο κόσκινο των Ερατοσθένη-Legendre, το οποίο μας δίνει έναν τύπο για τον υπολογισμό του $\pi(x)$ με γινόμενα

υπολογισμών που οδήγησαν στην πλήρη σχεδόν απόδειξη της αρχικής εικασίας του Waring και η τιμή της $g(\kappa)$ είναι πλέον γνωστό ότι δίνεται από την αναμενόμενη τιμή για αρκετά μεγάλα κ. Επιπλέον, για κάθε δοσμένο κ, είναι εύκολο να εξακριβωθεί η μέθοδος εύρεσης του $g(\kappa)$ από την εικασία, με τη μελέτη του κλασματικού μέρους του $\left(\frac{3}{2}\right)^{\kappa}$. Συνδυάζοντας τα αποτελέσματα αρκετών μαθηματικών, γνωρίζουμε πλέον ότι αν ισχύει ότι

$$1-\left\{\left(\frac{3}{2}\right)^{\kappa}\right\} \geq \left(\frac{3}{4}\right)^{\kappa},$$

όπου $\{\theta\}$ είναι το κλασματικό μέρος του θ, τότε ισχύει ο αναμενόμενος τύπος για το $g(\kappa)$. Αφού το δεξί μέλος της ανισότητας φθίνει εκθετικά ως προς κ, δεν είναι περίεργο να βρεθεί αντιπαράδειγμα για την ανισότητα αυτή. Ο K. Mahler απέδειξε το 1957 ότι υπάρχει το πολύ πεπερασμένο πλήθος τέτοιων αντιπαραδειγμάτων ή ακόμα και κανένα. Δυστυχώς, για τεχνικούς λόγους, ο προσδιορισμός του $g(\kappa)$ για κάθε κ, δεν έχει ακόμη αναχθεί σε πεπερασμένου πλήθους αριθμητικούς υπολογισμούς. Η τιμή του $g(\kappa)$ εξαρτάται κυρίως από την αναπαράσταση μερικών μικρών φυσικών αριθμών, αλλά η μελέτη των περιπτώσεων $\kappa = 4, 5$ δεν είναι καθόλου τετριμμένη. Ο J. R. Chen το 1963 και οι R. Balasubramanian και J. M. Deshouillers το 1989 απέδειξαν αντίστοιχα τα αναμενόμενα αποτελέσματα $g(5) = 37$ και $g(4) = 19$. Η έρευνα σήμερα σχετικά με το πρόβλημα του Waring περιορίζεται στην εκτίμηση του $G(\kappa)$, μόνο για $\kappa = 2$ και 4.

4.4 Η Μέθοδος του Κόσκινου

Στο 1ο Κεφάλαιο παρουσιάσαμε το κριτήριο της ρίζας το οποίο μπορεί να χρησιμοποιηθεί ως μέθοδος διαχωρισμού των πρώτων $p \leq x$ από τους σύνθετους, η οποία είναι γνωστή και ως **κόσκινο του Ερατοσθένη.** Η ιδέα είναι ότι η διαγραφή από μία λίστα με όλους τους αριθμούς έως τον x, των πολλαπλασίων όλων των πρώτων $p \leq \sqrt{x}$, οπότε οι εναπομείναντες αριθμοί θα είναι όλοι πρώτοι. Πολλές επεκτάσεις αυτής της μεθόδου είναι γνωστές και σε αυτή την ενότητα παρουσιάζουμε μερικές.

Ο Legendre το 1790 εφάρμοσε την αρχή Εγκλεισμού-Αποκλεισμού της Συνδυαστικής και οδηγήθηκε στο κόσκινο των Ερατοσθένη-Legendre, το οποίο μας δίνει έναν τύπο για τον υπολογισμό του $\pi(x)$ με γινόμενα

από αθροίσματα πρώτων $p \leq \sqrt{x}$. Ο τύπος αυτός ήταν ανεπαρκής όπως διεπίστωσε και ο ίδιος ο Legendre, δοκιμάζοντάς τον για διάφορες τιμές του $x \leq 400000$. Η δυσκολία έγκειται στο ότι υπάρχουν πάρα πολλοί όροι στον τύπο, για πρώτους $p \leq \sqrt{x}$. Το 1871 ο E. D. F. Meissel είχε την ιδέα να περιορισθούμε έως την $\sqrt[3]{x}$ και να δημιουργηθεί μία νέα διαδικασία απόρριψης των σύνθετων αριθμών που περισσεύουν.

Οι σύνθετοι αυτοί αριθμοί που θα είναι μικρότεροι του x, θα έχουν ακριβώς δύο πρώτους παράγοντες μεγαλύτερους του $\sqrt[3]{x}$, καθώς αν είχαν τρεις θα ξεπερνούσαν τον x. Ο Meissel χρησιμοποίησε τον τύπο του για να υπολογίσει τον $\pi(x)$ για $x = 10^6$, 10^7, 10^8 και 10^9, παρ' όλο που έκανε λάθος για την τελευταία τιμή.

Ο Meissel, όμως, ουσιαστικά τροποποίησε το άθροισμα του Legendre και απείχε ουσιαστικά από τη μορφή του κοσκίνου που αναπτύχθηκε κατά τη διάρκεια του αιώνα μας. Το 1920 ο V. Brun κατασκεύασε ένα κόσκινο χρησιμοποιώντας αρκετά αποτελέσματα της Συνδυαστικής. Το νέο στοιχείο είναι ότι το κόσκινο περιέχει παραμέτρους, οι οποίες δίνουν τη δυνατότητα επίτευξης άνω και κάτω φραγμάτων για το πλήθος των πρώτων που περιέχονται σε κάποιο διάστημα.

Με βάση αυτή την ιδέα, ο Brun απέδειξε ότι το πλήθος των διδύμων πρώτων μέχρι το x είναι το πολύ $Cx/(\log x)^2$ για κάποια σταθερά C. Δυστυχώς είναι πολύ δύσκολο να καταλήξουμε σε ικανοποιητικά κάτω φράγματα, και ακόμη δεν έχει αποδειχθεί ότι η συνάρτηση απαρίθμησης των δίδυμων πρώτων είναι μη φραγμένη. Ωστόσο, το προηγούμενο αποτέλεσμα οδήγησε στο ενδιαφέρον συμπέρασμα ότι το άθροισμα $\sum \frac{1}{p}$, με p να ανήκει στους δίδυμους πρώτους αποτελεί συγκλίνουσα σειρά, ενώ γνωρίζουμε ότι η αντίστοιχη σειρά για όλους τους πρώτους p είναι αποκλίνουσα.

Το 1950 απονεμήθηκε το Fields Medal στον A. Selberg για την εργασία του πάνω στη Θεωρία Αριθμών και ειδικότερα στον σχηματισμό του κόσκινου του Selberg. Εκτός του ότι ήταν απλούστερο στη χρήση από το κόσκινο του Brun, το νέο αυτό κόσκινο έδινε καλύτερα απότελέσματα, ειδικότερα όταν απαιτούνταν άνω φράγματα. Μάλιστα, η μέθοδος του Selberg οδηγούσε στα βέλτιστα άνω φράγματα, υπό την προϋπόθεση ότι κάποιες παράμετροι είναι δυνατόν να προσδιορισθούν. Παρ' όλο που η εύρεση κάτω φραγμάτων παρέμεινε δύσκολη, η μέθοδος του Selberg σε συνδυασμό με άλλες ιδιοφυείς παρατηρήσεις, οδήγησαν σε εντυπωσιακά αποτελέσματα, όπως το θώρημα του Chen για τους πρώτους, που είδαμε.

Τη δεκαετία του 1950, οι Yu.V. Linnik και A. Renyi έθεσαν τα θεμέλια για τη δημιουργία του "μεγάλου κόσκινου" των K. F. Roth κ.ά., στα τέλη της δεκαετίας του 1960. Το μέγαλο κόσκινο αποτελεί μία χρήσιμη ανισότητα που μας δίνει φράγματα για τη μέση τιμή και την τυπική απόκλιση της κατανομής των αριθμών σε διάφορες κλάσεις ισοϋπολοίπων. Το θεώρημα του Bombieri απετέλεσε τον προπομπό όλων αυτών των επιτευγμάτων.

4.5 Προσεγγιστικές μέθοδοι, Διοφαντικές εξισώσεις και υπερβατικοί αριθμοί

Σε αυτή την ενότητα θα παρουσιάσουμε τις εξελίξεις της Θεωρίας Αριθμών στον τομέα των προσεγγιστικών μεθόδων, των διοφαντικών εξισώσεων και των υπερβατικών αριθμών. Υπενθυμίζουμε ότι ένας αλγεβρικός αριθμός ν-οστού βαθμού είναι η ρίζα μίας πολυωνυμικής εξίσωσης ν-οστής τάξης με ακέραιους συντελεστές. Επομένως οι ρητοί αριθμοί είναι αλγεβρικοί αριθμοί πρώτου βαθμού, η χρυσή τομή $(1 + \sqrt{5})/2$ είναι αλγεβρικός αριθμός δευτέρου βαθμού. Υπερβατικός ονομάζεται ο αριθμός που δεν είναι αλγεβρικός.

4.5.1 Προσεγγίσεις αρρήτων με ρητούς

Έστω θ ένας άρρητος αριθμός. Για κάθε θετικό ακέραιο y, υπάρχει ακέραιος x έτσι ώστε το σφάλμα της ρητής προσέγγισης x/y του θ να ικανοποιεί τη σχέση:

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y}.$$

Πράγματι, αρκεί να θέσουμε $x = [y\theta]$, οπότε το $y\theta - x$ είναι το κλασματικό μέρος του $y\theta$, οπότε είναι μικρότερο του 1. Ένα ερώτημα που προκύπτει άμεσα είναι αν είναι δυνατό να αναζητήσουμε μία καλύτερη προσέγγιση, βρίσκοντας ένα καλύτερο φράγμα του σφάλματος για κατάλληλες τιμές του y. Με άλλα λόγια, υπάρχουν άπειρα κατάλληλα κλάσματα x/y, τέτοια ώστε

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y^x},$$

Τη δεκαετία του 1950, οι Yu.V. Linnik και A. Renyi έθεσαν τα θεμέλια για τη δημιουργία του "μεγάλου κόσκινου" των K. F. Roth κ.ά., στα τέλη της δεκαετίας του 1960. Το μέγαλο κόσκινο αποτελεί μία χρήσιμη ανισότητα που μας δίνει φράγματα για τη μέση τιμή και την τυπική απόκλιση της κατανομής των αριθμών σε διάφορες κλάσεις ισοϋπολοίπων. Το θεώρημα του Bombieri απετέλεσε τον προπομπό όλων αυτών των επιτευγμάτων.

4.5 Προσεγγιστικές μέθοδοι, Διοφαντικές εξισώσεις και υπερβατικοί αριθμοί

Σε αυτή την ενότητα θα παρουσιάσουμε τις εξελίξεις της Θεωρίας Αριθμών στον τομέα των προσεγγιστικών μεθόδων, των διοφαντικών εξισώσεων και των υπερβατικών αριθμών. Υπενθυμίζουμε ότι ένας αλγεβρικός αριθμός ν-οστού βαθμού είναι η ρίζα μίας πολυωνυμικής εξίσωσης ν-οστής τάξης με ακέραιους συντελεστές. Επομένως οι ρητοί αριθμοί είναι αλγεβρικοί αριθμοί πρώτου βαθμού, η χρυσή τομή $(1 + \sqrt{5})/2$ είναι αλγεβρικός αριθμός δευτέρου βαθμού. Υπερβατικός ονομάζεται ο αριθμός που δεν είναι αλγεβρικός.

4.5.1 Προσεγγίσεις αρρήτων με ρητούς

Έστω θ ένας άρρητος αριθμός. Για κάθε θετικό ακέραιο y, υπάρχει ακέραιος x έτσι ώστε το σφάλμα της ρητής προσέγγισης x/y του θ να ικανοποιεί τη σχέση:

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y}.$$

Πράγματι, αρκεί να θέσουμε $x = [y\theta]$, οπότε το $y\theta - x$ είναι το κλασματικό μέρος του $y\theta$, οπότε είναι μικρότερο του 1. Ένα ερώτημα που προκύπτει άμεσα είναι αν είναι δυνατό να αναζητήσουμε μία καλύτερη προσέγγιση, βρίσκοντας ένα καλύτερο φράγμα του σφάλματος για κατάλληλες τιμές του y. Με άλλα λόγια, υπάρχουν άπειρα κατάλληλα κλάσματα x/y, τέτοια ώστε

$$\left|\theta - \frac{x}{y}\right| < \frac{1}{y^x},$$

όπου $\varkappa$ δοσμένη παράμετρος μεγαλύτερη του 1. Όταν ισχύει το προηγούμενο, θα λέμε ότι το θ προσεγγίζεται στην τάξη $\varkappa$. Χρησιμοποιώντας ένα απλό επιχείρημα με βάση την αρχή της περιστεροφωλιάς, ο Dirichlet απέδειξε ότι κάθε άρρητος αριθμός προσεγγίζεται στην τάξη $\varkappa = 2$. Είναι όμως δυνατόν να έχουμε $\varkappa > 2$; Η απάντηση εξαρτάται από το θ, και ο Liouville το 1844, απέδειξε ότι ένας αλγεβρικός αριθμός δεν προσεγγίζεται σε τάξη $\varkappa$ μεγαλύτερη του βαθμού του. Ακριβέστερα, απέδειξε ότι αν ο θ είναι αλγεβρικός αριθμός βαθμού $\nu \geq 2$, τότε υπάρχει θετική σταθερά $c = c(\theta)$, τέτοια ώστε:

$$\left|\theta - \frac{x}{y}\right| > \frac{c}{y^{\nu}} \text{ για κάθε κλάσμα } \frac{x}{y}.$$

Ο Liouville χρησιμοποίησε το θεώρημά του για να κατασκευάσει αναλυτικά υπερβατικούς αριθμούς. Η ιδέα που χρησιμοποίησε ήταν ότι αν ένας αριθμός προσεγγίζεται σε αυθαίρετη τάξη, τότε δε μπορεί να είναι αλγεβρικός και έδωσε ως παράδειγμα έναν "αριθμό του Liouville" τον

$$\sum \frac{1}{10^{\nu!}}.$$

Αργότερα, ο Cantor το 1875 απέδειξε ότι σχεδόν όλοι οι αριθμοί είναι υπερβατικοί χωρίς να κατασκευάσει ουσιαστικά κανένα! Το ότι οι αριθμοί e και π είναι υπερβατικοί αποδείχθηκε από τον Hermite το 1881 και τον Lindermann το 1885 αντίστοιχα, οδηγώντας τον Hilbert να εισάγει δύο αντίστοιχα προβλήματα στα περίφημα 23 που πρότεινε για τον 20ο αιώνα.

Το θεώρημα του Dirichlet εκφράζει ότι το θεώρημα του Liouville ισχύει κατά βέλτιστο τρόπο όταν $\nu = 2$, ενώ όταν $\nu > 2$ είναι δυνατόν να γίνουν βελτιώσεις. Με άλλα λόγια, για έναν αλγεβρικό αριθμό θ βαθμού $\nu > 2$, και $2 < \varkappa < \nu$, αναρωτιόμαστε αν υπάρχει $c = c(\theta, \varkappa) > 0$ τέτοιο ώστε, για κάθε κλάσμα x/y, να έχουμε ότι:

$$\left|\theta - \frac{x}{y}\right| > \frac{c}{y^{\varkappa}}.$$

Ο A. Thue, το 1908, έδωσε μία πρώτη βελτίωση του θεωρήματος του Liouville αποδεικνύοντας την ύπαρξη των $c(\theta, \varkappa)$ όταν :

$$\frac{\nu}{2} + 1 < \varkappa < \nu.$$

Το θεώρημα του Thue βελτιώθηκε ακόμη από τους C. L. Siegel το 1921 και F. J. Dyson το 1947 σε $\kappa > 2\sqrt{\nu}$ και $\kappa > \sqrt{2\nu}$, αντίστοιχα. Το 1858 στον K. F. Roth απονεμήθηκε το Fields Medal για την ιδιοφυή του μέθοδο που οδήγησε στην εντυπωσιακή βελτίωση $\kappa > 2$ (1955), η οποία είναι η βέλτιστη κατά το θεώρημα του Dirichlet. Ωστόσο, η μέθοδος αυτή ασχολείται μόνο με την ύπαρξη και όχι με την κατασκευή του $c(\theta, \kappa)$.

4.5.2 Διοφαντικές εξισώσεις

Ο Thue συνειδητοποίησε ότι με μία βελτίωση του θεωρήματος του Liouville αποδεικνύεται ότι η διοφαντική εξίσωση:

$$\alpha_\nu x^\nu + \alpha_{\nu-1} x^{\nu-1} y + \ldots + \alpha_0 y^\nu = m,$$

όπου α_i, m είναι ακέραιοι και το πολυώνυμο είναι ανάγωγο, έχει πεπερασμένο το πλήθος λύσεις. Ο Thue απέδειξε μόνο ότι μία τέτοια εξίσωση έχει πεπερασμένο πλήθος λύσεων, χωρίς να καταφέρει να βρει φράγματα του πλήθους των λύσεων αυτών. Το στοιχείο αυτό έκανε δύσχρηστο το αποτέλεσμά του, για παράδειγμα μπορούμε να αποδείξουμε ότι μία διοφαντική εξίσωση έχει το πολύ δύο λύσεις, ενώ ουσιαστικά δεν έχει καμμία.

Στο 10ο πρόβλημα που πρότεινε ο Hilbert, ρωτούσε αν υπάρχει αλγόριθμος επίλυσης οποιασδήποτε πολυωνυμικής διοφαντικής εξίσωσης. Μετά από πάρα πολλές προσπάθειες–ξεχωρίζοντας την εργασία της J. Robinson στη δεκαετία του 1950–ο Yu. Matiyasevic (1970) απέδειξε ότι η απάντηση είναι αρνητική.

4.5.3 Υπερβατικοί αριθμοί

Το 7ο Πρόβλημα του Hilbert ασχολείται με την υπερβατικότητα διαφόρων αριθμών, όπως ο $e + \pi$, η σταθερά γ του Euler, καθώς επίσης και μία κλάση αριθμών της μορφής α^β, όπου α, β είναι αλγεβρικοί αριθμοί, με $\alpha \neq 0, 1$, και β άρρητο. Ειδικότερα, ο Hilbert ζητούσε την απόδειξη της υπερβατικότητας των $e^\pi = (-1)^i$ και $2^{\sqrt{2}}$, η οποία έγινε από τους A. O. Gelfond (1929) και K. Kusmin (1930), αντίστοιχα.

Η επίλυση του γενικότερου προβλήματος του α^β έγινε ανεξάρτητα από τους Gelfond και T. Schnieder το 1934. Το 1970 απονεμήθηκε το

Fields Medal στον Alan Baker για την εργασία του στη βελτίωση του θεωρήματος του Thue και τη γενίκευση του θεωρήματος των Gelfond-Schneider. Θεωρώντας γραμμικές μορφές με μεταβλητές λογαρίθμους, απέδειξε ότι αν οι $\alpha_1, \alpha_2, \ldots, \alpha_\nu$ είναι αλγεβρικοί αριθμοί, διάφοροι των 0 και 1, και $\beta_1, \beta_2, \ldots, \beta_\nu$ είναι αλγεβρικοί αριθμοί, οι οποίοι μαζί με το 1 είναι γραμμικά ανεξάρτητοι στο σύνολο των ρητών, τότε ο αριθμός $\alpha_1^{\beta_1} \cdot \alpha_2^{\beta_2} \cdot \ldots \cdot \alpha_\nu^{\beta_\nu}$ είναι υπερβατικός.

4.5.4 Σχετικά Αποτελέσματα

Ένα πολύ γνωστό αποτέλεσμα του Euler ήταν ότι:

$$\zeta(2) = \sum \frac{1}{\nu^2} = \frac{\pi^2}{6}$$

και η γενίκευσή του:

$$\zeta(2\nu) = |B_{2\nu}| \frac{(2\pi)^{2\nu}}{2 \cdot (2\nu)!},$$

όπου $B_{2\nu}$ είναι οι αριθμοί Bernoulli. Λίγα πράγματα ωστόσο είναι γνωστά για το $\zeta(2\nu + 1)$. Ο R. Apery το 1978 απέδειξε ότι ο $\zeta(3)$ είναι άρρητος. Ωστόσο, δεν υπάρχει ανάλογη απόδειξη για το $\zeta(5)$. Ένα εκπληκτικό αποτέλεσμα του K. Mahler το 1953 εκφράζει ότι:

$$\left|\pi - \frac{x}{y}\right| > \frac{1}{y^{42}}, \quad \gamma\iota\alpha\ y > 1.$$

Από αυτό προέκυψε το ερώτημα της εύρεσης της βέλτιστης τιμής του κ για την οποία η ανισότητα

$$\left|\pi - \frac{x}{y}\right| < \frac{1}{y^\kappa}$$

έχει πεπερασμένο πλήθος λύσεων. Πρόσφατα αποτελέσματα έδωσαν ως αποδεκτή λύση την $\kappa = 14$.

Όπως αναφέραμε προηγουμένως, θεωρώντας τα κλασματικά μέρη του $(3/2)^\kappa$, ο Mahler το 1957 απέδειξε επίσης ότι ο αναμενόμενος τύπος για την $g(\kappa)$ στο πρόβλημα του Waring ισχύει για αρκετά μεγάλες τιμές

του κ. Δυστυχώς, η απόδειξή του στηρίχθηκε σε μία παραλλαγή του θεωρήματος του Roth, οπότε το πρόβλημα του Waring δεν ανάγεται σε υπολογισμούς.

Ο R. Tijdeman το 1976 εφάρμοσε τη μέθοδο του Baker και βρήκε φράγματα του πλήθους των λύσεων αρκετών εκθετικών διοφαντικών εξισώσεων. Ειδικότερα, υπήρχε μία περίφημη εικασία του Catalan, ότι το 8 και το 9 είναι οι μοναδικοί διαδοχικοί αριθμοί, οι οποίοι είναι δυνάμεις φυσικών, οπότε οι αριθμοί $x = 3$, $y = 2$, $\alpha = 2$, $\beta = 2$ πρέπει να αποτελούν τη μοναδική λύση της εκθετικής διοφαντικής εξίσωσης:

$$x^{\alpha} = y^{\beta} + 1, \text{ όπου } \alpha > 1, \beta > 1.$$

Ο Tijdeman ανήγαγε την εικασία του Catalan σε απλή επαλήθευση με αριθμητικούς υπολογισμούς οι οποίοι ωστόσο είναι πάρα πολλοί.

4.6 Αριθμητικές συναρτήσεις και εκτιμήσεις εκθετικών αθροισμάτων

Πολλά προβλήματα της Θεωρίας Αριθμών ασχολούνται με τη συμπεριφορά διαφόρων αριθμητικών συναρτήσεων, όπως του μέγιστου πρώτου διαιρέτη ενός φυσικού ν ή του πλήθους των πρώτων διαιρετών του ν. Η μελέτη τέτοιων συναρτήσεων οδηγεί συχνά στην εκτίμηση εκθετικών αθροισμάτων η οποία αποτελεί σύγχρονο πεδίο έρευνας, όπως φαίνεται στο ακόλουθο παράδειγμα.

Έστω $\delta(\nu)$ το πλήθος των διαιρετών του ν. Η συμπεριφορά της συνάρτησης αυτής είναι ανορθόδοξη, π.χ. $\delta(p) = 2$, για p πρώτο, ενώ το $\delta(2^{\kappa}) = \kappa + 1$ γίνεται οσοδήποτε μεγάλο. Για να εξομαλύνουμε τις αποκλίσεις αυτές θεωρούμε τα αθροίσματα τα οποία εκφράζουν ότι η $\delta(\nu)$ έχει "μέση τιμή" κοντά στο $\log \nu$. Ειδικότερα, ο Dirichlet το 1841 απέδειξε ότι, όταν $x \to \infty$, τότε:

$$\sum_{\nu \leq x} \delta(\nu) = x \log x + (2\gamma - 1)x + O(\sqrt{x}),$$

όπου γ είναι η σταθερά του Euler.

Η απόδειξη βασίζεται στο γεγονός ότι το $\delta(\nu)$ είναι το πλήθος των λύσεων της εξίσωσης $\nu = \alpha\beta$, και το άθροισμα περικλείει τα συνδεσμικά

του κ. Δυστυχώς, η απόδειξή του στηρίχθηκε σε μία παραλλαγή του θεωρήματος του Roth, οπότε το πρόβλημα του Waring δεν ανάγεται σε υπολογισμούς.

Ο R. Tijdeman το 1976 εφάρμοσε τη μέθοδο του Baker και βρήκε φράγματα του πλήθους των λύσεων αρκετών εκθετικών διοφαντικών εξισώσεων. Ειδικότερα, υπήρχε μία περίφημη εικασία του Catalan, ότι το 8 και το 9 είναι οι μοναδικοί διαδοχικοί αριθμοί, οι οποίοι είναι δυνάμεις φυσικών, οπότε οι αριθμοί $x = 3$, $y = 2$, $\alpha = 2$, $\beta = 2$ πρέπει να αποτελούν τη μοναδική λύση της εκθετικής διοφαντικής εξίσωσης:

$$x^{\alpha} = y^{\beta} + 1, \text{ όπου } \alpha > 1, \beta > 1.$$

Ο Tijdeman ανήγαγε την εικασία του Catalan σε απλή επαλήθευση με αριθμητικούς υπολογισμούς οι οποίοι ωστόσο είναι πάρα πολλοί.

4.6 Αριθμητικές συναρτήσεις και εκτιμήσεις εκθετικών αθροισμάτων

Πολλά προβλήματα της Θεωρίας Αριθμών ασχολούνται με τη συμπεριφορά διαφόρων αριθμητικών συναρτήσεων, όπως του μέγιστου πρώτου διαιρέτη ενός φυσικού ν ή του πλήθους των πρώτων διαιρετών του ν. Η μελέτη τέτοιων συναρτήσεων οδηγεί συχνά στην εκτίμηση εκθετικών αθροισμάτων η οποία αποτελεί σύγχρονο πεδίο έρευνας, όπως φαίνεται στο ακόλουθο παράδειγμα.

Έστω $\delta(\nu)$ το πλήθος των διαιρετών του ν. Η συμπεριφορά της συνάρτησης αυτής είναι ανορθόδοξη, π.χ. $\delta(p) = 2$, για p πρώτο, ενώ το $\delta(2^{\kappa}) = \kappa + 1$ γίνεται οσοδήποτε μεγάλο. Για να εξομαλύνουμε τις αποκλίσεις αυτές θεωρούμε τα αθροίσματα τα οποία εκφράζουν ότι η $\delta(\nu)$ έχει "μέση τιμή" κοντά στο $\log \nu$. Ειδικότερα, ο Dirichlet το 1841 απέδειξε ότι, όταν $x \to \infty$, τότε:

$$\sum_{\nu \leq x} \delta(\nu) = x \log x + (2\gamma - 1)x + O(\sqrt{x}),$$

όπου γ είναι η σταθερά του Euler.

Η απόδειξη βασίζεται στο γεγονός ότι το $\delta(\nu)$ είναι το πλήθος των λύσεων της εξίσωσης $\nu = \alpha\beta$, και το άθροισμα περικλείει τα συνδεσμικά

σημεία (σημεία του επιπέδου με ακέραιες συντεταγμένες) (α, β) που ικανοποιούν ότι $\alpha\beta \leq x$. Με άλλα λόγια, το πρόβλημα αφορά στην εκτίμηση του πλήθους των συνδεσμικών σημείων που περιέχονται σε μία υπερβολή.

Οι αριθμοί οι οποίοι εκφράζονται ως άθροισμα δύο τετραγώνων είναι σπάνιοι, με την έννοια ότι σχηματίζουν ένα σύνολο μηδενικής πυκνότητας μέσα στο σύνολο των φυσικών. Δηλαδή, η εξίσωση $\nu = \alpha^2 + \beta^2$ είναι επιλύσιμη μόνο όταν ο ν ανήκει σε ένα ειδικό "λεπτό" σύνολο. Ωστόσο, όταν η εξίσωση αυτή είναι επιλύσιμη, τότε υπάρχει μεγάλο πλήθος δεκτών λύσεων (α, β). Αν $r(\nu)$ είναι το πλήθος των λύσεων αυτών, με $\alpha, \beta \in Z$, τότε το $r(\nu)$ είναι τις περισσότερες φορές 0, αλλά μερικές φορές παίρνει αρκετά μεγάλες τιμές. Η μέση τιμή του $r(\nu)$, βρίσκεται κοντά στο π! Πράγματι, ο Gauss απέδειξε ότι:

$$\sum_{\nu \leq x} r(\nu) = \pi x + O(\sqrt{x}).$$

Το άθροισμα αυτό εκφράζει τα συνδεσμικά σημεία (α, β) που ανήκουν μέσα στον κύκλο $\alpha^2 + \beta^2 \leq x$, με ακτίνα $\sqrt{x}$ και εμβαδόν πx. Δηλαδή ο όρος του σφάλματος αποτελεί τη διαφορά ανάμεσα στο εμβαδόν του κύκλου και το πλήθος των συνδεσμικών σημείων που περιέχει.

Ένα γενικό θεώρημα που ανέπτυξε ο M. V. Jarnik το 1928 εκφράζει ότι το πλήθος των συνδεσμικών σημείων που περιέχονται σε μία απλή, κλειστή καμπύλη διαφέρει από το εμβαδόν που περικλείει η καμπύλη αυτή, το πολύ όσο είναι το μήκος της. Ωστόσο, για τα δύο προηγούμενα προβλήματα οι καμπύλες που μελετήσαμε είναι ιδιαίτερα ομαλές, καθώς έχουν γνωστή καμπυλότητα και γεωμετρικές ιδιότητες που επιτρέπουν μία καλύτερη εκτίμηση σφάλματος από την $O(\sqrt{x})$.

Τα δύο ανωτέρω προβλήματα των Dirichlet και Gauss προσδιορίζουν τα μέγιστα κάτω φράγματα θ_o και θ_1 των συνόλων των τιμών του θ, για τις οποίες ισχύουν οι εκτιμήσεις σφάλματος $O(x^\theta)$ για τα προβλήματα αυτά. Επομένως, οι Dirichlet και Gauss απέδειξαν αντίστοιχα ότι $\theta_0, \theta_1 \leq \frac{1}{2}$, ενώ οι G. F. Voronoi και W. Sierpinski αντίστοιχα βελτίωσαν τις ανισότητες σε $\theta_0, \theta_1 \leq \frac{1}{3}$ το 1904.

Με τις βελτιώσεις αυτές, η μέθοδος απόδειξης τροποποιήθηκε σε προσεκτική αριθμητική ανάλυση με εκτιμήσεις αθροισμάτων κλασματικών μερών. Ουσιαστικά, μελετάμε αθροίσματα περιοδικών συναρτήσεων, οι οποίες αναλύονται σε τριγωνομετρικά ή εκθετικά αθροίσματα και οδηγούν σε σειρές Fourier.

Αρκετά προβλήματα της Θεωρίας Αριθμών, οδηγούν σε ασυμπτωτική ανάλυση, όπως τα προβλήματα των Goldbach και Waring. Για το λόγο αυτό, έχουν αναπτυχθεί αρκετές πολύπλοκες, αλλά ισχυρές μέθοδοι αντιμετώπισης προβλημάτων με εκθετικά αθροίσματα.

Εκτός από τη μέθοδο του Vinogradov και ο J.G. van der Corput το 1922, κατασκεύασε μία πολύ καλή μέθοδο που βελτίωσε τις εκτιμήσεις των θ_0 και θ_1, κάτω από το 1/3. Πολλές τέτοιες βελτιώσεις έχουν γίνει, έως την τελευταία το 1988 από τους H. Iwaniec και C.J. Mozzochi, που απέδειξαν ότι $\theta_1 \leq 7/22$. Είναι ενδιαφέρον, ότι κάθε νέο αποτέλεσμα για το ένα πρόβλημα, οδηγεί στο ίδιο αποτέλεσμα για το άλλο, παρόλο που κανείς δεν έχει αποδείξει ότι $\theta_0 = \theta_1$. Οι G. H. Hardy και E. Landau απέδειξαν ανεξάρτητα το 1914, ότι $\theta_0, \theta_1 \geq 1/4$ και εικάζεται ότι τελικά $\theta_0 = \theta_1 = 1/4$.

4.7 Υπολογιστική Θεωρία Αριθμών

Η Θεωρία Αριθμών αποτελεί πεδίο αριθμητικών πειραματισμών, καθώς πολλές εικασίες της έχουν διατυπωθεί μετά από πληθώρα αριθμητικών υπολογισμών. Με την ανάπτυξη της τεχνολογίας, καθώς και αντίστοιχων προγραμματιστικών πακέτων, η μελέτη μεγάλου πλήθους αριθμητικών δεδομένων, γίνεται ολοένα ευκολότερη και πιο αποτελεσματική. Η αλγεβρική Θεωρία Αριθμών έχει ευνοηθεί τα μέγιστα από τις υπολογιστικές μεθόδους. Η αναζήτηση μιας ικανής υπολογιστικής μεθόδου, συχνά οδηγεί στην κατανόηση ή ακόμη και επίλυση του δεδομένου προβλήματος. Για παράδειγμα, ας θεωρήσουμε τον ακόλουθο αλγόριθμο προσδιορισμού του αν ένας φυσικός $\nu > 1$ είναι πρώτος ή όχι. Χρησιμοποιώντας το κριτήριο της ρίζας, διαιρούμε διαδοχικά τον ν με έναν διαιρέτη δ που παίρνει τις τιμές $\delta = 2, 3, \ldots$, μέχρι να βρεθεί διαιρέτης, οπότε θα ξέρουμε ότι ο ν είναι πρώτος αν δεν έχει διαιρέτη έως ότου $\delta^2 > \nu$.

Αν ο ν είναι σύνθετος, τότε ο προηγούμενος αλγόριθμος υπολογίζει επιπλέον τον ελάχιστο πρώτο διαιρέτη του ν. Δυστυχώς, ο αλγόριθμος αυτός είναι πρακτικά αδύνατος για μεγάλες τιμές του ν. Ένα θεμελιώδες πρόβλημα στη Θεωρία Αριθμών είναι κατά πόσο υπάρχει "εφικτός" αλγόριθμος για το πρόβλημα αυτό. Ο όρος "εφικτός" ωστόσο πρέπει να προσδιορισθεί με ακρίβεια.

Αρκετά προβλήματα της Θεωρίας Αριθμών, οδηγούν σε ασυμπτωτική ανάλυση, όπως τα προβλήματα των Goldbach και Waring. Για το λόγο αυτό, έχουν αναπτυχθεί αρκετές πολύπλοκες, αλλά ισχυρές μέθοδοι αντιμετώπισης προβλημάτων με εκθετικά αθροίσματα.

Εκτός από τη μέθοδο του Vinogradov και ο J.G. van der Corput το 1922, κατασκεύασε μία πολύ καλή μέθοδο που βελτίωσε τις εκτιμήσεις των θ_0 και θ_1, κάτω από το 1/3. Πολλές τέτοιες βελτιώσεις έχουν γίνει, έως την τελευταία το 1988 από τους H. Iwaniec και C.J. Mozzochi, που απέδειξαν ότι $\theta_1 \leq 7/22$. Είναι ενδιαφέρον, ότι κάθε νέο αποτέλεσμα για το ένα πρόβλημα, οδηγεί στο ίδιο αποτέλεσμα για το άλλο, παρόλο που κανείς δεν έχει αποδείξει ότι $\theta_0 = \theta_1$. Οι G. H. Hardy και E. Landau απέδειξαν ανεξάρτητα το 1914, ότι $\theta_0, \theta_1 \geq 1/4$ και εικάζεται ότι τελικά $\theta_0 = \theta_1 = 1/4$.

4.7 Υπολογιστική Θεωρία Αριθμών

Η Θεωρία Αριθμών αποτελεί πεδίο αριθμητικών πειραματισμών, καθώς πολλές εικασίες της έχουν διατυπωθεί μετά από πληθώρα αριθμητικών υπολογισμών. Με την ανάπτυξη της τεχνολογίας, καθώς και αντίστοιχων προγραμματιστικών πακέτων, η μελέτη μεγάλου πλήθους αριθμητικών δεδομένων, γίνεται ολοένα ευκολότερη και πιο αποτελεσματική. Η αλγεβρική Θεωρία Αριθμών έχει ευνοηθεί τα μέγιστα από τις υπολογιστικές μεθόδους. Η αναζήτηση μιας ικανής υπολογιστικής μεθόδου, συχνά οδηγεί στην κατανόηση ή ακόμη και επίλυση του δεδομένου προβλήματος. Για παράδειγμα, ας θεωρήσουμε τον ακόλουθο αλγόριθμο προσδιορισμού του αν ένας φυσικός $\nu > 1$ είναι πρώτος ή όχι. Χρησιμοποιώντας το κριτήριο της ρίζας, διαιρούμε διαδοχικά τον ν με έναν διαιρέτη δ που παίρνει τις τιμές $\delta = 2, 3, \ldots$, μέχρι να βρεθεί διαιρέτης, οπότε θα ξέρουμε ότι ο ν είναι πρώτος αν δεν έχει διαιρέτη έως ότου $\delta^2 > \nu$.

Αν ο ν είναι σύνθετος, τότε ο προηγούμενος αλγόριθμος υπολογίζει επιπλέον τον ελάχιστο πρώτο διαιρέτη του ν. Δυστυχώς, ο αλγόριθμος αυτός είναι πρακτικά αδύνατος για μεγάλες τιμές του ν. Ένα θεμελιώδες πρόβλημα στη Θεωρία Αριθμών είναι κατά πόσο υπάρχει "εφικτός" αλγόριθμος για το πρόβλημα αυτό. Ο όρος "εφικτός" ωστόσο πρέπει να προσδιορισθεί με ακρίβεια.

Ας θεωρήσουμε έναν αλγόριθμο Α, ο οποίος φέρνει αποτέλεσμα μετά από συγκεκριμένους υπολογισμούς για δοσμένη τιμή του ν. Εχοντας υπόψη ότι ο αριθμός ν έχει $N = \log \nu$ ψηφία, τα οποία προσδιορίζουν ακριβώς τον ν, θα λέμε ότι ο Α είναι αλγόριθμος **πολυωνυμικού χρόνου** αν περατώνει με ακρίβεια τη συγκεκριμένη διαδικασία μετά από N^K το πολύ πράξεις, για δοσμένο K. Το ερώτημα είναι αν υπάρχει αλγόριθμος πολυωνυμικού χρόνου, για τη διάκριση των πρώτων από τους σύνθετους. Αν η δοσμένη τιμή του ν είναι πρώτος, τότε ο προηγούμενος αλγόριθμος απαιτεί τουλάχιστον $\sqrt{\nu}$ πράξεις, προτού τερματισθεί. Αφού

$$\sqrt{\nu} = e^{\left(\frac{1}{2}ln\nu\right)} = e^{\frac{N}{2}},$$

θα λέμε ότι είναι αλγόριθμος **εκθετικού χρόνου.**

Ο καλύτερος αλγόριθμος που υπάρχει στις ημέρες μας είναι των L. M. Adleman, C. Pomerance και R. S. Rumeley, το 1983, ο οποίος είναι–χωρίς να είναι ακριβώς–αλγόριθμος πολυωνυμικού χρόνου. Ο αλγόριθμος αυτός τερματίζεται μετά από το πολύ:

$$(\log \nu)^{c \log(\log(\log \nu))} = N^{c \log(\log N)}$$

βήματα όπου c είναι μία θετική σταθερά. Η βασική ιδέα του αλγορίθμου αυτού χρησιμοποιεί τις αρχικές ρίζες των πρώτων και μπορεί με άνεση να εξετάσει αν ένας φυσικός εκατοντάδων ψηφίων είναι πρώτος ή όχι.

Το συναφές πρόβλημα της παραγοντοποίησης ενός φυσικού ν είναι πολύ πιο δύσκολο, ιδιαίτερα αν αναζητήσουμε έναν αλγόριθμο, ο οποίος δεν θα τερματίσει, παρά μόνο όταν ολοκληρωθεί η παραγοντοποίηση. Αν ισχυρισθούμε ότι ένας αριθμός δ διαιρεί έναν φυσικό ν, αρκεί με μία διαίρεση να το επαληθεύσουμε, οπότε απαιτείται αλγόριθμος πολυωνυμικού χρόνου. Έτσι, είναι καλύτερο να οδηγηθούμε σε αλγορίθμους, στους οποίους "μαντεύουμε" τους διαιρέτες ενός αριθμού. Φυσικά, η μέθοδος αυτή παρουσιάζει δυσκολίες διαφορετικής υφής.

Σχεδόν όλοι οι αλγόριθμοι παραγοντοποίησης είναι αυτής της μορφής και μπορούμε να περιγράψουμε έναν από τους πιο απλούς, αυτόν που ανέπτυξε ο J. M. Pollard το 1975:
Έστω ν ένας αρκετά μεγάλος σύνθετος αριθμός ($\nu \approx 10^{30}$), του οποίου θέλουμε να βρούμε τον ελάχιστο πρώτο διαιρέτη p. Σχηματίζουμε μία ακολουθία αριθμών $x_0, x_1, \ldots,$ οι οποίοι είναι διακεκριμένοι $(mod \nu)$, αλλά όχι διακεκεριμένοι $(mod p)$. Απλούστερα, θέτουμε $x_0 = 2$ και $x_{j+1} \equiv$

$x_j^2 + 1(mod\nu)$. Αν $x_i \equiv x_j(modp)$, τότε ο μέγιστος κοινός διαιρέτης $(x_i - x_j, \nu)$ είναι ένας μη-τετριμμένος διαιρέτης του ν, και ο πρώτος διαιρέτης p προσδιορίζεται από τον Ευκλείδειο αλγόριθμο. Αρκεί, λοιπόν, να βρούμε μόνο το μέγιστο κοινό διαιρέτη $(x_{2\varkappa} - x_\varkappa, \nu)$ για $\varkappa = 1, 2, 3, \ldots$, και μπορούμε να πετύχουμε ότι $\varkappa \approx \sqrt{p}$.

Ιδιαίτερο ενδιαφέρον σε αλγόριθμους εύρεσης πρώτων και παραγοντοποίησης παρουσιάσθηκε λόγω της ανάπτυξης της σύγχρονης θεωρίας της Κρυπτογραφίας ανοιχτού κλειδιού. Αν η παραγοντοποίηση ενός αριθμού ν είναι ιδιαίτερα δύσκολη, τότε είναι δυνατόν να κατασκευάσουμε μονόδρομες συναρτήσεις $\nu \longrightarrow f(\nu)$ στις οποίες ο υπολογισμός του $f(\nu)$ είναι εύκολος, αλλά η αντίστροφη διαδικασία εύρεσης του ν από το $f(\nu)$ είναι πρακτικά αδύνατη. Μπορούμε τότε να κατασκευάσουμε μηνύματα με ένα γνωστό σε όλους κλειδί, τα οποία για να αποκρυπτογραφηθούν θα πρέπει να γνωρίζει κάποιος ένα κρυφό κλειδί, αδύνατο να υπολογισθεί από τους υπόλοιπους. Ένα από τα πλέον σύγχρονα και διάσημα κρυπτογραφικά συστήματα είναι το RSA,που αναπτύχθηκε το 1978, από τους R. L. Rivest, A. Shamir και L. M. Adleman. Στο σύστημα αυτό εκμεταλλευόμαστε κυρίως την αδυναμία μας να παραγοντοποιήσουμε έναν σχετικά μεγάλο αριθμό. Η δυσκολία της παραγοντοποίησης είναι φανερή στο ακόλουθο παράδειγμα:
Έστω $N = pq,\ p \leq q$ πρώτοι.
Γνωρίζοντας τις δυαδικές γραφές των p και q, μπορούμε να βρούμε τον N κάνοντας $\varkappa(\log q)^2$ πράξεις, όπου $\varkappa$ σταθερά. Αντίθετα, αν γνωρίζαμε τον N και ψάχναμε τους πρώτους παράγοντές του χρειάζονται (υποθέτοντας ότι ελέγχουμε όλους τους φυσικούς $\leq \sqrt{N}$)

$$\varkappa'\sqrt{N} = \varkappa' e^{\frac{1}{2}lnN}$$

πράξεις, δηλαδή πολύ περισσότερες. Ακόμα και αν χρησιμοποιήσουμε γρηγορότερους αλγορίθμους παραγοντοποίησης, η παραγοντοποίηση παραμένει ένα δύσκολο πρόβλημα, και, ιδίως αν ο αριθμός έχει λίγους πρώτους παράγοντες, είναι πρακτικά αδύνατη για μεγάλους ακεραίους. Αυτές οι τεχνικές έχουν μέχρι σήμερα πολλές εφαρμογές σε τραπεζικά συστήματα, στο διαδίκτυο κ.α.

Στο κρυπτοσύστημα RSA ο Α διαλέγει δύο μεγάλους πρώτους p, q (με περίπου 80–100 ψηφία) και υπολογίζει τον $N = pq$.

Στη συνέχεια διαλέγει έναν αριθμό e με

$$\left\{ \begin{array}{rl} (e, N) & = 1 \\ (e, \varphi(N)) & = 1 \end{array} \right\}$$

και γνωστοποιεί σε όλους το ζεύγος: (N, e). Αν ο B θέλει να στείλει στον A ένα μήνυμα M (ένα θετικό ακέραιο) υπολογίζει το :

$$K = K(M) = M^e (mod N) \quad (\text{κωδικοποιημένο μήνυμα})$$

Ο A για να αποκωδικοποιήσει το μήνυμα, έχει υπολογίσει εκ των προτέρων, τον αριθμό x έτσι ώστε

$$ex \equiv 1 mod(\varphi(N)), \quad \text{όπου } \varphi(N) = (p-1)(q-1)$$

και υπολογίζει το

$$\begin{aligned} K^{-1}(K(M)) = K^x (mod N) &\equiv M^{ex} (mod N) \\ &\equiv M^{1+\varphi(N)\alpha} (mod N) \\ &\equiv M (mod N) \end{aligned}$$

δηλαδή $K^{-1}(M) = M^x (mod N)$. Για τον προσδιορισμό του x είναι απαραίτητη η γνώση του $\varphi(N)$, που για $N = pq$ είναι ισοδύναμο πρόβλημα με την παραγοντοποίηση του N. Έτσι μόνο ο A που γνωρίζει την παραγοντοποίηση του N μπορεί να αποκωδικοποιήσει το μήνυμα.

Επιπλέον εκτός από την ασφάλεια που παρέχει, ο αλγόριθμος αυτός παρέχει δύο επιπλέον στοιχεία που χαρακτηρίζουν ένα καλό κρυπτοσύστημα:

- Πιστοποίηση ταυτότητας αποστολέα.
- Δυνατότητα απόδειξης ότι ο αποστολέας έστειλε το μήνυμα.

Η διαφορά μεταξύ των δύο είναι ότι στην πρώτη περίπτωση αρκεί ο A να πείσει τον εαυτό του ότι το μήνυμα ήρθε όντως από τον B, ενώ στη δεύτερη περίπτωση ο A μπορεί να αποδείξει (να πείσει κάποιον δικαστή) ότι ο B απέστειλε το μήνυμα–ο B δηλαδή δε μπορεί να αρνηθεί ότι το μήνυμα ήρθε από αυτόν. Αυτό μπορεί να γίνει ως εξής:

Ο Β μπορεί να συμπεριλάβει στο τέλος του μηνύματός του μία "υπογραφή" Y, την οποία κωδικοποιεί ως:

$$K_A(K_B^{-1}(Y))$$

όπου K_A είναι ο αλγόριθμος κωδικοποίησης του Α και K_B^{-1} ο αλγόριθμος αποκωδικοποίησης του Β. Ο Α αποκωδικοποιώντας το μήνυμά του, βρίσκει το $K_B^{-1}(Y)$. Γνωρίζοντας ότι το μήνυμα φαινομενικά προήλθε από τον Β, εφαρμόζει το K_B (το οποίο ο Β έχει κάνει γνωστό σε όλους) οπότε παίρνει

$$K_A(K_B^{-1}(Y)) = Y.$$

Κανένας άλλος δε θα μπορούσε να στείλει το σωστό $K_A(K_B^{-1}(Y))$, αφού μόνο ο Β γνωρίζει το K_B^{-1}. Επίσης, ο Β δε μπορεί να αρνηθεί ότι ήταν αυτός που έστειλε το $K_A(K_B^{-1}(Y))$. Επιπλέον ο Β δεν αποκαλύπτει καμμία πληροφορία για το κλειδί του φανερώνοντας το $K_B^{-1}(Y)$ στον Α.

Βέβαια, αν $N_B > N_A$ το $K_A(K_B^{-1}(Y))$ δεν υπάρχει απαραίτητα (καθώς το σύνολο τιμών του $K_B^{-1}(X)$ είναι μεγαλύτερο από το πεδίο ορισμού του $K_A(X)$–δηλαδή ο Β έχει μεγαλύτερο "αλφάβητο" από τον Α), αλλά σε αυτή την περίπτωση ο Β μπορεί να στείλει ως υπογραφή το

$$K_B^{-1}(K_A(Y))$$

οπότε ο Α εφαρμόζει πρώτα το K_B (που είναι γνωστό σε όλους) και μετά το K_A^{-1} (που μόνο αυτός ξέρει) και παίρνει την υπογραφή Y.

Στην πράξη χρησιμοποιούνται βελτιωμένες παραλλαγές του RSA που παρέχουν μεγαλύτερη ασφάλεια, (π.χ.κάποιος τρίτος μπορεί να πάρει πληροφορίες για τη δομή του N μελετώντας στατιστικά πόση ώρα χρειάζεται για να κωδικοποιηθεί ένα μήνυμα ή μπορεί να καταφέρει να "κλέψει" την υπογραφή κάποιου άλλου κατά την αποστολή).

Τέλος, απαιτείται ιδιαίτερη προσοχή στην επιλογή των p, q, οι οποίοι θα πρέπει να είναι όσο το δυνατόν "τυχαίοι" γίνεται, δηλαδή να μην είναι μιας συγκεκριμένης μορφής (π.χ. πρώτοι του Mersenne κ.λπ.). Ένας ικανοποιητικά καλός τρόπος εύρεσης τέτοιων πρώτων είναι να διαλέξουμε τυχαία ένα μεγάλο περιττό x και αν είναι σύνθετος να ελέγξουμε στη συνέχεια τον $x + 2$ κ.λπ. μέχρι να βρούμε έναν πρώτο.

Επίσης, η υπογραφή Y θα πρέπει να είναι συνάρτηση του μηνύματος M, ώστε ο Α να μη μπορεί να προσποιηθεί στον Γ ότι είναι ο Β

κατασκευάζοντας το

$$K_\Gamma(K_B^{-1}(Y))$$

και στέλνοντας ένα μήνυμα στον Γ.

Με αλγόριθμους που χρησιμοποιούν "μονόδρομες συναρτήσεις" γίνεται η κωδικοποίηση των προσωπικών αριθμών των τραπεζικών καρτών και των αριθμών πρόσβασης στα δίκτυα UNIX (Internet). Δηλαδή όταν κάποιος βάζει κάποιον αριθμό ως κωδικό, το σύστημα κωδικοποιεί τον αριθμό και τον συγκρίνει με τον κωδικοποιημένο αριθμό που υπάρχει ήδη πάνω στην κάρτα ή σε κάποιο αρχείο. Η αντίστροφη διαδικασία δηλαδή από τον κωδικοποιημένο αριθμό να βρεθεί ο αρχικός είναι σχεδόν αδύνατη, δεδομένου επίσης του ότι οι τράπεζες αλλάζουν τον αλγόριθμο κωδικοποίησης κατά τακτά χρονικά διαστήματα.

Τα τελευταία χρόνια, ιδιαίτερο ενδιαφέρον παρουσιάζει η κατασκευή ενός "κβαντικού υπολογιστή", ο οποίος θα χρησιμοποιεί ιδιότητες των στοιχειωδών σωματιδίων να "θυμούνται" όλες τις καταστάσεις από τις οποίες πέρασε το σωματίδιο. Με έναν τέτοιο υπολογιστή, προβλήματα τα οποία είναι δύσκολα με έναν συνηθισμένο υπολογιστή που λειτουργεί με βάση την αρχή του Turing είναι πολύ εύκολα και αντίστροφα. Προβλήματα τα οποία θα μπορούν να λυθούν γρήγορα με ένα κβαντικό υπολογιστή είναι αυτά της παραγοντοποίησης ακεραίων και ερωτήματα, όπως το αν το επίπεδο μπορεί να καλυφθεί πλήρως από δοσμένα γεωμετρικά σχήματα. Στην πράξη, για να διαπιστώσουμε σήμερα κάτι τέτοιο "κατασκευάζουμε" τα σχήματα βιολογικά χρησιμοποιώντας βάσεις DNA οι οποίες ενώνονται μεταξύ τους με συγκεκριμένους τρόπους και προσπαθούμε να τα "αναγκάσουμε" να απλωθούν στο επίπεδο.

Παράδειγμα Κρυπτογραφικού Συστήματος

A	B	Γ	Δ	E	Z	H	Θ	I	K	Λ	M	N	Ξ
00	01	02	03	04	05	06	07	08	09	10	11	12	13
O	Π	P	Σ	T	Y	Φ	X	Ψ	Ω	$<$ κενό $>$	!	?	
14	15	16	17	18	19	20	21	22	23	24	25	26	

Επιλέγουμε $p = 47$, $q = 59$, $N = pq = 2773$. (στην πράξη χρησιμοποιούνται πολύ μεγαλύτεροι αριθμοί) και $e = 5$. Δημοσιοποιούμε το ζεύγος $(2773, 3)$.

Έστω ότι καποιος θέλει να μας στείλει το παρακάτω μήνυμα:

Γ	E	I	A
02	04	08	00

Κωδικοποιούμε ξεχωριστά τους αριθμούς 0204 και 0800:
0204:

$$\begin{aligned} 204^5(mod2773) &\equiv 204 \cdot (204^2)^2(mod2773) \\ &\equiv 204 \cdot 21^2(mod2773) \\ &\equiv 204 \cdot 441(mod2773) \\ &\equiv 1228(mod2773) \end{aligned}$$

0800:

$$\begin{aligned} 800^5(mod2773) &\equiv 800 \cdot (800^2)^2(mod2773) \\ &\equiv 800 \cdot (-563)^2(mod2773) \\ &\equiv 800 \cdot 847(mod2773) \\ &\equiv 0998(mod2773) \end{aligned}$$

Έτσι ο αποστολέας μας στέλνει την ακολουθία :

12280998.

Για να αποκωδικοποιήσουμε το μήνυμα προσδιορίζουμε τον x ώστε

$$ex \equiv 1(mod(p-1)(q-1)) \text{ ή}$$

$$5x \equiv 1(mod2668)$$

η οποία έχει λύση (βλ. Κεφ. 2) $x \equiv 1601(mod2668)$.
Έτσι έχουμε

$$\begin{aligned} 1228^{1601}(mod2773) &\equiv 1228 \cdot (-528)^{800}(mod2773) \\ &\equiv 1228 \cdot (1484)^{400}(mod2773) \\ &\equiv 1228 \cdot (494)^{200}(mod2773) \\ &\equiv 1228 \cdot (12)^{100}(mod2773) \\ &\equiv 1228 \cdot (1325)^{25}(mod2773) \\ &\equiv 1228 \cdot (1325 \cdot 316^2)^5(mod2773) \\ &\equiv 1228 \cdot (1051)^5(mod2773) \\ &\equiv (1228 \cdot 1051) \cdot 947^2(mod2773) \\ &\equiv 1183 \cdot 1130(mod2773) \\ &\equiv 204(mod2773) \end{aligned}$$

Όμοια υπολογίζουμε ότι $998^{1601} \equiv 800(mod 2773)$ οπότε το αποκρυπτογραφημένο μήνυμα είναι :

$$02\dot{:}04\dot{:}08\dot{:}00 \quad = \Gamma EIA.$$

4.8 Το μεγάλο Θεώρημα του Fermat

Τέλος καμμία ανασκόπηση της Θεωρίας Αριθμών δεν μπορεί να μην αναφερθεί στο μεγάλο Θεώρημα του Fermat το οποίο απέκτησε τη φήμη του παραμένοντας άλυτο για αιώνες. Η μελέτη του διάσημου αυτού προβλήματος της Θεωρίας Αριθμών ξεκίνησε από το γνωστό Πυθαγόρειο Θεώρημα:

$$x^2 + y^2 = z^2.$$

Οι Πυθαγόρειοι είχαν μελετήσει την ύπαρξη ακεραίων τριάδων (x, y, z) που ικανοποιούν το παραπάνω πρόβλημα. Οι ακέραιες λύσεις της εξίσωσης αυτής είναι καταγεγραμμένες στα "Στοιχεία" του Ευκλείδη και αργότερα χρησιμοποιήθηκαν και από τον Διόφαντο στην γνωστή μας μορφή:

$$x = \mu^2 - \nu^2,\ y = 2\mu\nu \ \textit{και}\ z = \mu^2 + \nu^2$$

όπου μ, ν φυσικοί. Είναι προφανές ότι μπορούμε να πολλαπλασιάσουμε τα x, y, z με μία ακέραια παράμετρο t για να πετύχουμε όλες τις δυνατές ακέραιες λύσεις της εξίσωσης.

Η μελέτη του Πυθαγορείου Θεωρήματος επεκτάθηκε αρχικά σε διάφορες παραλλαγές σχετικές με επιμέρους ιδιότητες των αριθμών μίας Πυθαγόρειας τριάδας, έως το 1637, οπότε ο Pierre Fermat διετύπωσε την εικασία ότι:

"Είναι αδύνατη η ανάλυση κύβου σε άθροισμα δύο κύβων, διτετράγωνου σε άθροισμα δύο διτετράγωνων και γενικότερα οποιουδήποτε ακεραίου υψωμένου στη ν-οστή δύναμη σε άθροισμα δύο ακεραίων υψωμένων στον ίδιο εκθέτη (με $\nu > 2$)."

Η περίφημη αυτή εικασία ονομάσθηκε "Μεγάλο Θεώρημα" του Fermat, η οποία συμπληρωνόταν από την ιδιόχειρη φράση του:

"Ανακάλυψα μία εξαιρετική απόδειξη αλλά δεν είναι αρκετό το περιθώριο για να την καταγράψω".

Ο Fermat δεν άφησε στα χειρόγραφά του την πλήρη απόδειξη της εικασίας του, ενώ συχνά αναφερόταν στην αλληλογραφία του για τις περιπτώσεις του κύβου και του διτετράγωνου. Την τελευταία είχε αποδείξει με τη **μέθοδο της άπειρης καθόδου**.

Η απόδειξη για τους κύβους έγινε το 1755 από τον L. Euler, ο οποίος προηγουμένως (1747) είχε αποδείξει και την περίπτωση των διτετράγωνων. Οι H. S. Germain, ο A. M. Legendre και τελικά ο P. G. L. Dirichlet

απέδειξαν το θεώρημα του Fermat για $\nu = 5$ με προσπάθειες που διήρκησαν έως το 1825. Το 1832 ο Dirichlet απέδειξε και την περίπτωση $\nu = 14$, ενώ ο G. Lamé το 1839 απέδειξε την περίπτωση $\nu = 7$. Αρκετοί ήταν οι μαθηματικοί που υποστήριξαν λανθασμένα, ότι απέδειξαν πλήρως το θεώρημα του Fermat. Ο Lamé το 1847 παρουσίασε μία απόδειξη, η οποία αναιρέθηκε από τους Liouville και E. E. Kummer. Ο τελευταίος ωστόσο παρουσίασε το 1847 μία απόδειξη για κανονικούς πρώτους (τους πρώτους που δεν διαιρούν τους αριθμητές των ρητών αριθμών Bernoulli B_ν).

Πολλοί ερευνητές προσπάθησαν να αποδείξουν το Θεώρημα του Fermat για τους πρώτους που δεν είναι κανονικοί, έως ότου ο Jensen το 1915 απέδειξε ότι οι μη-κανονικοί πρώτοι είναι άπειροι. Με βάση τα αριθμητικά δεδομένα ωστόσο υπήρχαν σοβαρές ενδείξεις ότι ισχύει το θεώρημα του Fermat, η επαλήθευσή του είχε φτάσει έως την τιμή $\nu = 4000000$. Ένα σημαντικό αποτέλεσμα ανέπτυξε το 1983 ο G. Faltings, όταν απέδειξε ότι υπάρχει το πολύ πεπερασμένο πλήθος πρώτων x, y, z που ικανοποιούν την εξίσωση $x^\nu + y^\nu = z^\nu$, για οποιοδήποτε εκθέτη $\nu > 2$.

Ο Frey το 1986 ήταν αυτός που συνέδεσε ουσιαστικά το θεώρημα Fermat με την εικασία των Taniyama-Shimura-Weil, η οποία στηριζόταν σε δύο ανοιχτά προβλήματα της θεωρίας ελλειπτικών καμπυλών και την οποία απέδειξε ο A. Wiles το 1993 για μία ειδική κλάση παραδειγμάτων ικανή να οδηγήσει στην απόδειξη του Θ. Fermat. Η τελική απόδειξη του θεωρήματος Fermat δημοσιεύθηκε το 1995, μετά από κάποιες επιπλέον διορθώσεις στις σελίδες 443–551 του τεύχους 142 του επιστημονικού μαθηματικού περιοδικού "Annals of Mathematics".

Λύσεις Ασκήσεων

Λύσεις Ασκήσεων §1.1

Α' Ομάδα

1. (i) $100 = 5 \cdot 17 + 15$
   (ii) $-100 = (-6)17 + 2$
   (iii) $289 = 17 \cdot 17 + 0$
   (iv) $-342 = (-21)17 + 15$

2. Έστω οι ακέραιοι α και β. Διακρίνουμε περιπτώσεις ανάλογα με την αρτιότητά τους:

   (i) Αν είναι άρτιοι, δηλαδή $\alpha = 2\kappa$ και $\beta = 2\lambda$, τότε το γινόμενό τους $\alpha \cdot \beta = 4\kappa\lambda$ είναι άρτιος.

   (ii) Αν είναι περιττοί, δηλαδη, $\alpha = 2\kappa + 1$ και $\beta = 2\lambda + 1$, τότε το γινόμενό τους $\alpha \cdot \beta = 4\kappa\lambda + 2\lambda + 2\kappa + 1 =$
   $= 2(2\kappa\lambda + \lambda + \kappa) + 1$ είναι περιττός.

   (iii) Αν είναι διαφορετικής αρτιότητας, δηλαδή $\alpha = 2\kappa$ και $\beta = 2\lambda + 1$, τότε το γινόμενό τους
   $\alpha \cdot \beta = 4\kappa\lambda + 2\kappa = 2(2\kappa\lambda + \kappa)$ είναι άρτιος.

   Επομένως, το γινόμενο δύο ακεραίων είναι περιττός αριθμός αν και μόνο αν οι ακέραιοι αυτοί είναι περιττοί.

3. (i) Η απόδειξη είναι άμεση από την προηγούμενη άσκηση.
   (ii) Προφανές, από το (i).

4. (i) Έστω $\alpha = 4\mu + 1$ και $\beta = 4\lambda + 1$, δύο ακέραιοι.
   Τότε $\alpha \cdot \beta = (4\mu + 1)(4\lambda + 1) = 16\mu\lambda + 4\mu + 4\lambda + 1$, δηλαδή $\alpha \cdot \beta = 4(4\mu\lambda + \mu + \lambda) + 1$.
   (ii),(iii) Όμοια με (i).

5. Έστω ο ακέραιος $\nu = 6\kappa + 5$. Είναι προφανές ότι

$$\nu = 3 \cdot 2 \cdot \kappa + (6 - 1) = 3(2\kappa + 1) - 1.$$

Για το αντίστροφο, θεωρούμε τον ακέραιο $\nu = 3\kappa - 1$ και αν ο αριθμός κ είναι περιττός, τότε $\nu = 3(2\lambda+1)-1 = 6\lambda+3-1 = 6\lambda+2$. Επομένως, το αντίστροφο δεν ισχύει γενικά.

6. Κάθε φυσικός $\alpha = 8\kappa + 5$, γράφεται
$$\alpha = 4(2\kappa) + 4 + 1 = 4(2\kappa + 1) + 1,$$
δηλαδή στη μορφή $\alpha = 4\lambda + 1$, με $\lambda = 2\kappa + 1$.
Το αντίστροφο δεν ισχύει, διότι για παράδειγμα, ο αριθμός $9 = 4\cdot 2+1$ δεν γράφεται στη μορφή $9 = 8\kappa+5$ για κάποιο φυσικό κ.

7. Ο ακέραιος α είναι της μορφής $\alpha = 16\nu + 11$.
Ο αριθμός $\alpha + 3 = 16\nu + 14$ διαιρούμενος με τον β=16 αφήνει υπόλοιπο υ=14.
Ο αριθμός $\alpha + 5 = 16\nu + 16 = 16(\nu + 1)$ διαιρούμενος με τον β=16 αφήνει υπόλοιπο υ=0.
Όμοια εργαζόμαστε και στις υπόλοιπες περιπτώσεις.

8. Έχουμε διαδοχικά $\nu^2 = (5\kappa + 1)^2 = 25\kappa^2 + 10\kappa + 1 = 5(5\kappa^2 + 2\kappa) + 1$.

9. Κάθε ακέραιος ν γράφεται ν=3ρ ή ν=3ρ+1 ή ν=3ρ+2. Ελέγχουμε ξεχωριστά κάθε περίπτωση.
   (i) Αν ν=3ρ , τότε $\nu^2 = 9\rho^2$.
   (ii) Αν ν=3ρ+1 , τότε $\nu^2 = (3\rho + 1)^2 = 3(3\rho^2 + 2\rho) + 1$.
   (iii) Αν ν=3ρ+2 , τότε $\nu^2 = (3\rho + 2)^2 = 3(3\rho^2 + 4\rho + 1) + 1$.

10. Η λύση είναι προφανής από την προηγούμενη άσκηση.

11. Διακρίνουμε περιπτώσεις:
   (i) Αν $\nu = 5\kappa$, τότε $\nu^2 = 5(5\kappa^2)$.
   (ii) Αν $\nu = 5\kappa + 1$, τότε $\nu^2 = 5(5\kappa^2 + 2\kappa) + 1$.
   (iii) Αν $\nu = 5\kappa + 2$, τότε $\nu^2 = 5(5\kappa^2 + 4\kappa) + 4$.
   (iv) Αν $\nu = 5\kappa + 3$, τότε $\nu^2 = 5(5\kappa^2 + 6\kappa + 1) + 4$.
   (v) Αν $\nu = 5\kappa + 4$, τότε $\nu^2 = 5(5\kappa^2 + 8\kappa + 3) + 1$.

Β' Ομάδα

12. Ο N είναι περιττός αν και μόνο αν οι παράγοντες $\alpha-\beta$, $\beta-\gamma$ και $\gamma-\alpha$ είναι περιττοί. Δηλαδή, καθένας από τους ακεραίους α, β, και γ πρέπει να είναι διαφορετικής αρτιότητας με τους υπόλοιπους δύο. Αυτό είναι αδύνατο, οπότε ο αριθμός N είναι άρτιος.

13. Έστω δύο περιττοί $\alpha = 2\nu+1$ και $\beta = 2\kappa+1$.
Έχουμε $\alpha^2+\beta^2 = (2\nu+1)^2+(2\kappa+1)^2 = 4\nu^2+4\nu+1+4\kappa^2+4\kappa+1$, δηλαδή $\alpha^2+\beta^2 = 2[2(\nu^2+\nu+\kappa^2+\kappa)+1]$.Ο αριθμός $N = \alpha^2+\beta^2$ δεν είναι τέλειο τετράγωνο ακεραίου καθώς είναι γινόμενο του 2 και του περιττού αριθμού $2(\nu^2+\nu+\kappa^2+\kappa)+1$.

14. Ένας ακέραιος ν γράφεται στη μορφή ν=3ρ ή ν=3ρ+1 ή ν=3ρ+2.
Ελέγχουμε ξεχωριστά κάθε περίπτωση :

(i) αν ν=3ρ, τότε $\nu^3 = 27\rho^3 = 9(3\rho^3)$,
(ii) αν ν=3ρ+1, τότε $\nu^3 = 27\rho^3+27\rho^2+9\rho+1 =$
$= 9(3\rho^3+3\rho^2+\rho)+1$,
(iii) αν ν=3ρ+2, τότε $\nu^3 = 27\rho^3+54\rho^2+36\rho+8 =$
$= 9(3\rho^3+6\rho^2+4\rho)+8$.

15. Έστω ν και ν+1 δύο διαδοχικοί ακέραιοι. Τότε

$$(\nu+1)^3-\nu^3 = \nu^3+3\nu^2+3\nu+1-\nu^3 = 3\nu(\nu+1)+1,$$

όπου ο ακέραιος 3ν(ν+1) είναι άρτιος.
Άρα ο $(\nu+1)^3-\nu^3$ είναι περιττός.

16. Ας θεωρήσουμε έναν φυσικό αριθμό $\nu = \kappa^2 = \mu^3$.
Ελέγχοντας ξεχωριστά τις περιπτώσεις:

$$\kappa = 7\rho \text{ ή } 7\rho+1 \text{ ή } 7\rho+2 \text{ ή} \ldots \text{ ή } 7\rho+6 \quad \text{και}$$
$$\mu = 7\tau \text{ ή } 7\tau+1 \text{ ή } 7\tau+2 \text{ ή} \ldots \text{ ή } 7\tau+6$$

καταλήγουμε στο ζητούμενο αποτέλεσμα.

17. Για περιττό ακέραιο $\alpha = 2\kappa+1$ έχουμε ότι

$$\begin{aligned}\alpha^4 &= (2\kappa+1)^4\\ &= (4\kappa^2+4\kappa+1)^2\\ &= 8\kappa(2\kappa^3+4\kappa^2+3\kappa+1)+1.\end{aligned}$$

Ένας από τους αριθμούς x και $2x^3+4x^2+3x+1$ θα είναι άρτιος. Άρα ο α^4 γράφεται

$$\begin{aligned}\alpha^4 &= 16\left[\frac{x(2x^3+4x^2+3x+1)}{2}\right]+1\\ &= 16\mu+1,\end{aligned}$$

όπου ο $\mu=\frac{x(2x^3+4x^2+3x+1)}{2}$ είναι ακέραιος.

18. Προφανώς, αν οι αριθμοί x, y είναι της ίδιας αρτιότητας, τότε το άθροισμα x^2+y^2 είναι άρτιος άρα $x^2+y^2\neq 1999$.
Ας υποθέσουμε ότι $x=2\kappa+1$ και $y=2\lambda$.
Τότε,

$$\begin{aligned}x^2+y^2 &= 4\kappa^2+4\kappa+1+4\lambda^2\\ &= 4(4\kappa^2+\kappa+\lambda^2)+1\end{aligned}$$

και αφού ο αριθμός $1999=4\cdot 499+3$ δεν είναι της μορφής $4\mu+1$, έχουμε ότι $x^2+y^2\neq 1999$, για κάθε ακεραίους x, y.

19. Αν θεωρήσουμε έναν περιττό ακέραιο x, τότε το άθροισμα $N=x^\nu+x^{\nu-1}+\ldots+x^2+x$ αποτελείται από άρτιο πλήθος περιττών όρων, άρα ο N είναι άρτιος. Αν θεωρήσουμε έναν άρτιο x, τότε προφανώς το άθροισμα $N=x^\nu+x^{\nu-1}+\ldots+x^2+x$ είναι άρτιος αριθμός. Και στις δύο περιπτώσεις ο αριθμός $x^\nu+x^{\nu-1}+\ldots+x^2+x+\alpha$ είναι περιττός.

20. Το τελευταίο ψηφίο ενός φυσικού ν είναι το υπόλοιπο της διαίρεσής του με τον αριθμό 10. Διακρίνουμε περιπτώσεις:

    (i) Αν $\nu=10\kappa$, τότε $\nu^2=100\kappa^2$ και το τελευταίο ψηφίο του ν^2 είναι 0.

    (ii) Αν $\nu=10\kappa+1$, τότε $\nu^2=10(10\kappa^2+2\kappa)+1$ και το τελευταίο ψηφίο του ν^2 είναι 1.

    (iii) Αν $\nu=10\kappa+2$, τότε $\nu^2=10(10\kappa^2+4\kappa)$ και το τελευταίο ψηφίο του ν^2 είναι 4.

    ⋮

    (x) Αν $\nu=10\kappa+9$, τότε $\nu^2=10(10\kappa^2+18\kappa)+81=$
    $=10(10\kappa^2+18\kappa+8)+1$ και το τελευταίο ψηφίο του ν^2 είναι 1.

Λύσεις Ασκήσεων § 1.2

Α' Ομάδα

1. Απλή εφαρμογή του ορισμού.

2. (i) $N = 10000/5 = 2000$
   (ii) $N = 10000/25 = 400$
   (iii) $N = 10000/125 = 80$
   (iv) $N = 9900/225 = 44$.

3. (i) $N = (994 - 98)/7 = 128$
   (ii) $N = (986 - 85)/17 = 53$
   (iii) $N = (999 - 81)/27 = 34$
   (iv) $N = (980 - 98)/49 = 18$.

4. Έστω οι αριθμοί $\alpha = 6$, $\beta = 3$ και $\gamma = 4$. Τότε $6 \mid 3 \cdot 4$ ενώ $6 \nmid 3$ και $6 \nmid 4$.
   Άρα υπάρχουν θετικοί ακέραιοι α, β, γ με $\alpha \mid \beta \cdot \gamma$, $\alpha \nmid \beta$ και $\alpha \nmid \gamma$.

5. Αφού $\alpha \mid \beta$, υπάρχει ακέραιος λ τέτοιος ώστε $\beta = \lambda\alpha$. Για κάθε θετικό ακέραιο κ, έχουμε ότι $\beta^\kappa = \lambda^\kappa \cdot \alpha^\kappa$, οπότε $\alpha^\kappa \mid \beta^\kappa$.

6. (i) Αν $\alpha \mid \beta$ και $\alpha \mid \gamma$, τότε υπάρχουν ακέραιοι μ και ν τέτοιοι ώστε $\beta = \mu\alpha$ και $\gamma = \nu\alpha$. Άρα $\beta\gamma = \nu\mu\alpha^2$ και $\alpha^2 \mid \beta\gamma$.
   (ii) Αν $\alpha \mid \beta$ και $\gamma \neq 0$ τότε υπάρχει ακέραιος ν τέτοιος ώστε $\beta = \nu\alpha$ ή $\alpha\beta = \nu\alpha\gamma$, δηλαδή $\alpha\gamma \mid \beta\gamma$.
   Αντίστροφα, αν $\alpha\gamma \mid \beta\gamma$ και $\gamma \neq 0$, τότε υπάρχει ακέραιος ν τέτοιος ώστε $\beta\gamma = \nu\alpha\gamma$. Άρα $\beta = \nu\alpha$ και $\alpha \mid \beta$.

7. Αφού ο α δεν είναι πολλαπλάσιο του 2 ή του 3 θα γράφεται στη μορφή $\alpha = 6\kappa \pm 1$. Επομένως

$$\alpha^2 = 36\kappa^2 \pm 12\kappa + 1 = 12(3\kappa^2 \pm \kappa) + 1.$$

8. (i) Εχουμε ότι :

$$\begin{aligned} 2^{2\nu} - 1 &= 4^\nu - 1 = (4-1)(4^{\nu-1} + 4^{\nu-2} + \ldots + 4 + 1) \\ &= 3(4^{\nu-1} + 4^{\nu-2} + \ldots + 4 + 1). \end{aligned}$$

(ii) Είναι :

$$\alpha^\nu - \beta^\nu = (\alpha - \beta)(\alpha^{\nu-1} + \alpha^{\nu-2}\beta + \ldots + \alpha\beta^{\nu-2} + \beta^{\nu-1}).$$

(iii) Εχουμε ότι :

$$\alpha^{2\nu-1} + \beta^{2\nu-1} = (\alpha + \beta)(\alpha^{2\nu-2} - \alpha^{2\nu-3}\beta + \ldots - \alpha\beta^{2\nu-3} + \beta^{2\nu-2}).$$

9. Έχουμε ότι

$$\begin{aligned}\alpha^{2\nu} - \beta^{2\nu} &= (\alpha^2)^\nu - (\beta^2)^\nu \\ &= (\alpha^2 - \beta^2)(\alpha^{2(\nu-1)} + \alpha^{2(\nu-2)}\beta^2 + \ldots + \beta^{2(\nu-1)}) \\ &= (\alpha + \beta)(\alpha - \beta)(\alpha^{2(\nu-1)} + \alpha^{2(\nu-2)}\beta^2 + \ldots + \beta^{2(\nu-1)}).\end{aligned}$$

10. Γνωρίζουμε ότι ο αριθμός ν^2 είναι της μορφής $5\mu + 1$ ή $5\mu + 4$. Αν $\nu^2 = 5\mu + 1$, τότε $\nu^4 = (5\mu + 1)^2 = 5(5\mu^2 + 2\mu) + 1$, ενώ αν $\nu^2 = 5\mu + 4$, τότε $\nu^4 = (5\mu + 4)^2 = 5(5\mu^2 + 8\mu + 3) + 1$.

11. Έχουμε ότι $\alpha^2 = 5\kappa \pm 1$ και $\beta^2 = 5\lambda \pm 1$. Επομένως

$$\begin{aligned}\alpha^4 - \beta^4 &= 25\kappa^2 \pm 10\kappa + 1 - 25\lambda^2 \pm 10\lambda - 1 \\ &= 5(5\kappa^2 \pm 2\kappa - 5\lambda^2 \pm 2\lambda).\end{aligned}$$

Β' Ομάδα

12. Έχουμε

$$\begin{aligned}N &= 2 + 2^2 + 2^3 + 2^4 + \ldots + 2^{\nu-1} + 2^\nu \\ &= 2 + 2^2 + 2^2(2 + 2^2) + \ldots + 2^{\nu-2}(2 + 2^2) \\ &= 6 + 2^2 \cdot 6 + \ldots + 2^{\nu-2} \cdot 6 \\ &= 6(1 + 2^2 + \ldots + 2^{\nu-2}).\end{aligned}$$

Επομένως $6 \mid N$.

13. Έστω α ένας ακέραιος, ο οποίος είναι πολλαπλάσιο του 3 αλλά όχι και του 2. Τότε ο αριθμός α γράφεται στη μορφή $\alpha=6\kappa+1$ ή $\alpha=6\kappa+3$ ή $\alpha=6\kappa+5$.

(i)Αν $\alpha=6\kappa+1$, τότε $\alpha^2 - 1 = (6\kappa + 1)^2 - 1 = 4(9\kappa^2 + 3\kappa)$.

(ii)Αν $\alpha=6\kappa+3$, τότε $\alpha^2 - 1 = (6\kappa+3)^2 - 1 = 4(9\kappa^2 + 9\kappa + 6)$.

(iii)Αν $\alpha=6\kappa+5$, τότε $\alpha^2 - 1 = (6\kappa+5)^2 - 1 = 4(9\kappa^2 + 15\kappa + 6)$.

14. Ο αριθμός $N = 2^{4\nu+2} + 1$ γράφεται

$$\begin{aligned} N &= 4^{2\nu+1} + 1 \\ &= (4+1)(4^{2\nu} + 4^{2\nu-1} + \ldots + 4 + 1) \\ &= 5(4^{2\nu} + 4^{2\nu-1} + \ldots + 4 + 1) \end{aligned}$$

Άρα ο αριθμός

$$\frac{2^{4\nu+2}+1}{5} = 4^{2\nu} + 4^{2\nu-1} + \ldots + 4 + 1$$

είναι ακέραιος.

15. Αφού οι α, β δεν είναι πολλαπλάσια του 3, της μορφής $\alpha = 3\kappa \pm 1$ και $\beta = 3\lambda \pm 1$. Επομένως,

$$\begin{aligned} N &= \alpha^2 + \beta^2 = (3\kappa \pm 1)^2 + (3\lambda \pm 1)^2 \\ &= 9\kappa^2 \pm 6\kappa + 1 + 9\lambda^2 \pm 6\lambda + 1 \\ &= 3(3\kappa^2 \pm 2\kappa + 3\lambda^2 \pm 2\lambda) + 2. \end{aligned}$$

Είναι φανερό ότι ο N αποκλείεται να είναι τέλειο τετράγωνο ακεραίου.

16. Προφανώς στο γινόμενο $(4\nu)! = 1 \cdot 2 \cdot 3 \cdot 3 \cdot \ldots \cdot \nu \cdot (\nu+1) \cdot \ldots \cdot 4\nu$ έχουμε 2ν άρτιους παράγοντες, από τους οποίους ν παράγοντες είναι πολλαπλάσια του 4.
Άρα ισχύει $(\underbrace{2 \cdot 2 \cdot \ldots \cdot 2}_{\nu-\text{φορές}} \cdot \underbrace{4 \cdot 4 \cdot \ldots \cdot 4}_{\nu-\text{φορές}}) \mid (4\nu)!$, δηλαδή $8^\nu \mid (4-\nu)!$
Επιπλέον, για τον $(6\nu)! = (4\nu)! \cdot (4\nu+1)(4\nu+2) \cdot \ldots \cdot 6\nu$ είναι φανερό ότι είναι πολλαπλάσιο του 8^ν και έχει ν άρτιους παράγοντες στο γινόμενο $(4\nu+1)(4\nu+2)\ldots(6\nu)$. Άρα $2^\nu 8^\nu \mid (6\nu)!$ ή $16^\nu \mid (6\nu)!$.

17. Ο αριθμός N γράφεται

$$N = \nu(\nu^2-1)(\nu^2+1) = \nu(\nu-1)(\nu+1)(\nu^2+1).$$

Αν $\nu = 5\kappa$ ή $\nu = 5\kappa+1$ ή $\nu = 5\kappa+4$, τότε ένας από τους ν, $\nu-1$, $\nu+1$ θα είναι πολλαπλάσιο του 5 και η απόδειξη ολοκληρώθηκε.
Αν $\nu = 5\kappa+2$, τότε ο αριθμός $\nu^2+1 = 5(5\kappa^2+4\kappa+1)$ είναι πολλαπλάσιο του 5.

Αν $\nu = 5\kappa + 3$, τότε ο αριθμός $\nu^2 + 1 = 5(5\kappa^2 + 6\kappa + 2)$ είναι πολλαπλάσιο του 5.
Άρα ο αριθμός $N = \nu^5 - \nu$ διαιρείται τέλεια με τον αριθμό 5, για κάθε φυσικό ν.

18. Έστω οι διαδοχικοί ακέραιοι $\nu - 1$, ν, $\nu + 1$. Το άθροισμα των κύβων τους είναι

$$\begin{aligned} N &= (\nu-1)^3 + \nu^3 + (\nu+1)^3 \\ &= \nu^3 - 3\nu^2 + 3\nu - 1 + \nu^3 + \nu^3 + 3\nu^2 + 3\nu + 1 \\ &= 3\nu^3 + 6\nu \\ &= 3\nu(\nu^2 + 2). \end{aligned}$$

Διακρίνουμε περιπτώσεις:

(i) αν $\nu = 3\kappa$, τότε $N = 9\kappa(9\kappa^2 + 2)$,
(ii) αν $\nu = 3\kappa + 1$, τότε $N = 3(3\kappa + 1)3(3\kappa^2 + 2\kappa + 1)$,
(iii)αν $\nu = 3\kappa + 2$, τότε $N = 3(3\kappa + 2)3(3\kappa^2 + 2\kappa + 2)$.

Άρα πάντα ο αριθμός N είναι πολλαπλάσιο του 9.

19. Αφού $\kappa > \nu$ θα έχουμε ότι $\kappa = \nu + \mu$. Τότε

$$\begin{aligned} \alpha^{2^\kappa} - 1 &= (\alpha^{2^{\nu+1}})^{2^{\mu-1}} - 1 \\ &= [(\alpha^{2^\nu})^2 - 1] \cdot (\ldots) \\ &= (\alpha^{2^\nu} - 1)(\alpha^{2^\nu} + 1)(\ldots) \end{aligned}$$

και $(\alpha^{2^\nu} - 1) \mid (\alpha^{2^\kappa} - 1)$. Άρα $\delta \mid \alpha^{2^\kappa} - 1$ και $\delta \mid (\alpha^{2^\kappa} + 1)$, δηλαδή $\delta \mid 2$.
Αν ο αριθμός α είναι άρτιος, τότε ο $\alpha^{2^\nu} - 1$ είναι περιττός και $\delta = 1$.
Αν ο αριθμός α είναι περιττός, τότε ο $\alpha^{2^\nu} - 1$ είναι άρτιος και $\delta = 2$.

20. Για $\alpha \geq 2$ έχουμε

$$(\alpha - 1)\alpha(\alpha + 1) = \alpha(\alpha^2 + \kappa) - (\kappa + 1)\alpha,$$

οπότε συμπεραίνουμε ότι ο $\alpha^2 + \kappa$ διαιρεί τον $(\kappa + 1)\alpha$, άρα

$$\begin{aligned} \alpha^2 + \kappa &\leq (\kappa + 1)\alpha \\ \text{ή} \quad \alpha(\alpha - 1) &\leq \kappa(\alpha - 1) \\ \text{ή} \quad \alpha &\leq \kappa. \end{aligned}$$

Αν $\alpha = 1$ τότε προφανώς $\kappa \geq 1$ από την υπόθεση.

21. Ας υποθέσουμε ότι $x = \nu y$, με $\nu > 1$. Επειδή και οι δύο αριθμοί είναι επταψήφιοι, θα πρέπει $\nu < 10$. Οι αριθμοί x, y έχουν άθροισμα ψηφίων

$$1 + 2 + 3 + 4 + 5 + 6 + 7 = 28$$

οπότε αφήνουν υπόλοιπο 1 διαιρούμενοι με το 9, δηλαδή $y = 9\varkappa + 1$ για κάποιο $\varkappa$.
Όμως τότε $\nu y = 9\nu\varkappa + \nu$ και επειδή ο x αφήνει υπόλοιπο 1 με το 9 πρέπει $\nu = 1$, δηλ. $x = y$, άτοπο. Άρα ο x δεν είναι πολλαπλάσιο του y.

22. Παρατηρούμε ότι

$$2304 = 2^8 \cdot 3^2 = (2^4 \cdot 3)^2 = 48^2.$$

Ακόμη

$$\begin{aligned} 7^{2\nu} - 2352\nu - 1 &= (7^2)^\nu - 2352\nu - 1 \\ &= (1 + 48)^\nu - 48\nu - 1 - 2304\nu \\ &= \binom{\nu}{2} \cdot 48^2 + \binom{\nu}{3} \cdot 48^3 + \ldots + 48^\nu - 2304\nu \\ &= 2304 \cdot \left[\binom{\nu}{2} + \binom{\nu}{3} \cdot 48 + \ldots + 48^{\nu-2} - \nu\right]. \end{aligned}$$

Άρα $2304 \mid N$.

23. Αν $\mu > 2$, τότε από τη σχέση $2^\nu = \alpha^\mu - 1$ έχουμε

$$2^\nu = (\alpha - 1)(\alpha^{\mu-1} + \alpha^{\mu-2} + \ldots + \alpha + 1).$$

Ο ακέραιος α αποκλείεται να είναι άρτιος, διότι τότε το δεύτερο μέλος της ισότητας θα ήταν περιττός αριθμός, άτοπο.
Άρα ο ακέραιος α είναι περιττός. Επιπλέον ο $\alpha - 1$ πρέπει να είναι δύναμη του 2, δηλαδή $\alpha - 1 = 2^\varkappa$ ή $\alpha = 2^\varkappa - 1$ $(\varkappa\mu < \nu)$.
Όμως

$$\begin{aligned} \alpha^\mu &= 2^\nu + 1, \\ (2^\varkappa - 1)^\mu &= 2^\nu + 1, \\ 2^{\varkappa\mu} + \mu 2^{\varkappa(\mu-1)} + \ldots + \mu 2^\varkappa &= 2^\nu, \end{aligned}$$

που είναι αληθές μόνο για $\mu = 2$, $\varkappa = 1$, $\alpha = 3$ και $\nu = 3$.

Λύσεις Ασκήσεων § 1.3

Α' Ομάδα

1. Αν $x = (2\nu - 1, 2\nu + 1)$ τότε ο αριθμός x διαιρεί τέλεια την διαφορά $(2\nu + 1) - (2\nu - 1) = 2$.
   Άρα $x = 1$ ή $x = 2$ και αφού οι αριθμοί $2\nu + 1$ και $2\nu - 1$ είναι περιττοί καταλήγουμε στο ότι x=1.

2. Ανάμεσα σε τρεις διαδοχικούς φυσικούς $\nu, \nu + 1, \nu + 2$ θα υπάρχει τουλάχιστον ένας από αυτούς που είναι άρτιος και ένας ακριβώς που είναι πολλαπλάσιο του 3.
   Επειδή (2,3)=1, παίρνουμε ότι $6 = 2 \cdot 3 \mid \nu(\nu + 1)(\nu + 2)$.

3. Όμοια με την προηγούμενη άσκηση.

4. $(1109, 4999) = 1, \ \ (2318, 1769) = 29.$

5. $(-2353)(1109)+(522)(4999) = 1, \ \ (13)(2318)+(-17)(1769) = 29.$

6. Προφανώς, αν $\delta = (\alpha, \beta)$ τότε $\delta \mid (\alpha + \beta)$, $\delta \mid (\alpha - \beta)$ και $\delta \leq (\alpha + \beta, \alpha - \beta)$.

7. Αν θέσουμε $\delta = (\alpha, \alpha + \nu)$, τότε $\delta \mid \alpha$ και $\delta \mid (\alpha + \nu)$. Άρα $\delta \mid [(\alpha + \nu) - \alpha]$, δηλαδή $\delta \mid \nu$.

8. Αφού $(\nu, \nu + x) = 1$, θα έχουμε ότι $(\nu, x) = 1$ για κάθε φυσικό ν. Επιλέγοντας $\nu = x$ προκύπτει ότι $(x, x) = 1$, άρα $x = 1$ ή -1.

9. Αν ο μέγιστος κοινός διαιρέτης δύο φυσικών ν και x είναι (ν,x)=3, τότε $3 \mid (\nu + x)$ και αποκλείεται να ισχύει ν+x=100, διότι ο αριθμός 100 δεν είναι πολλαπλάσιο του 3.

10. Αποδεικνύονται άμεσα και οι τρεις ιδιότητες από την Εφ. 8 § 1.3.

Β' Ομάδα

11. Αν για έναν τυχαίο ακέραιο κ θεωρήσουμε τον $\delta = (\alpha, \beta) = (14\kappa + 3, 21\kappa + 1)$, τότε $\delta \mid (14\kappa + 3)$, $\delta \mid (21\kappa + 1)$, οπότε $\delta \mid [3 \cdot (14\kappa + 3) - 2(21\kappa + 1)]$.
Άρα $\delta \mid 7$ και αφού $\delta \mid (21\kappa + 1)$, έχουμε ότι $\delta \mid [21\kappa + 1 - 7(3\kappa)]$, δηλαδή $\delta \mid 1$ συνεπώς $\delta = 1$.

12. Έστω τρεις ακέραιοι αριθμοί α, β και γ τέτοιοι ώστε $(\alpha, \beta) = (\beta, \gamma) = (\alpha, \gamma) = 1$.

(i) Από τη σχέση $(\alpha, \beta) = 1$, θα υπάρχουν ακέραιοι x, y τέτοιοι ώστε $\alpha x + \beta y = 1$, άρα $\alpha\gamma x + \beta\gamma y = \gamma$. Αν $\delta = (\alpha, \beta, \gamma)$, τότε $\delta \mid \alpha$ και $\delta \mid \gamma$. Επομένως, $\delta \mid (\alpha, \gamma)$ και $\delta = 1$.

(ii)Για τους ακέραιους α^κ, β^ν και γ^μ ισχύει $(\alpha^\kappa, \beta^\nu) = (\beta^\nu, \gamma^\mu) = 1$ και από το ερώτημα (i) προκύπτει άμεσα ότι $(\alpha^\kappa, \beta^\nu \cdot \gamma^\mu) = 1$.

13. Έστω α και β δύο φυσικοί με $(\alpha, \beta)=1$ και $\delta = (\alpha + \beta, \alpha - \beta)$. Προφανώς ο δ διαιρεί το άθροισμα $(\alpha + \beta) + (\alpha - \beta) = 2\alpha$ και τη διαφορά $(\alpha + \beta) - (\alpha - \beta) = 2\beta$. Άρα $\delta \mid (2\alpha, 2\beta)$ και $\delta \mid 2$, αφού $(\alpha, \beta) = 1$, οπότε $\delta = 1$ ή $\delta = 2$.

14. Έστω $(\alpha, \beta)=1$ και $(\alpha + \kappa\beta, \beta)=\delta$ για έναν τυχαίο ακέραιο κ. Τότε $\delta \mid \beta$ και $\delta \mid (\alpha+\kappa\beta)$, άρα $\delta \mid [(\alpha+\kappa\beta)-\kappa\beta]$, οπότε $\delta \mid \alpha$. Επομένως, $\delta \mid (\alpha, \beta)$, δηλαδή $\delta = 1$.

15. (i) Αν $\delta = (8\alpha + 5, 5\alpha + 3)$, τότε $\delta \mid (8\alpha + 5)$ και $\delta \mid (5\alpha + 3)$.
Άρα $\delta \mid [5(8\alpha + 5) - 8(5\alpha + 3)]$, δηλαδή $\delta \mid 1$ και $\delta = 1$.

(ii) Έστω $\delta_1 = (\alpha, \beta)$ και $\delta_2 = (\alpha - \beta, 2\alpha - 3\beta)$.
Αφού $\delta_1 \mid \alpha$ και $\delta_1 \mid \beta$, έχουμε ότι $\delta_1 \mid (\alpha - \beta)$ και $\delta_1 \mid (2\alpha - 3\beta)$, άρα $\delta_1 \leq \delta_2$.
Αφού $\delta_2 \mid (\alpha - \beta)$ και $\delta_2 \mid (2\alpha - 3\beta)$ είναι φανερό ότι $\delta_2 \mid [2(\alpha-\beta) - (2\alpha-3\beta)]$, άρα $\delta_2 \mid \beta$ και $\delta_2 \mid [3(\alpha-\beta) - (2\alpha-3\beta)]$, δηλαδή $\delta_2 \mid \alpha$.
Επομένως, $\delta_2 \leq \delta_1$ οπότε $\delta_1 = \delta_2$.

16. (i) Χρησιμοποιώντας την Πρόταση 1.3.2 έχουμε:

$$\begin{aligned}(\alpha+\beta,\, 5\alpha+6\beta) &= (\alpha+\beta,\, 5\alpha+6\beta-5(\alpha+\beta))\\ &= (\alpha+\beta,\, \beta)\\ &= (\alpha+\beta-\beta,\, \beta)\\ &= (\alpha,\, \beta).\end{aligned}$$

(ii) Έστω $\delta_1 = (2\alpha+3\beta,\, 3\alpha+4\beta)$ και $\delta_2 = (\alpha,\beta)$
Αφού $\delta_2 \mid \alpha$ και $\delta_2 \mid \beta$, από το Θεώρημα 1.2.1 έχουμε ότι
$\delta_2 \mid (2\alpha+3\beta)$ και $\delta_2 \mid (3\alpha+4\beta)$, άρα $\delta_2 \leq \delta_1$.
Αφού $\delta_1 \mid (2\alpha+3\beta)$ και $\delta_1 \mid (3\alpha+4\beta)$, έχουμε ότι
$\delta_1 \mid [3(2\alpha+3\beta)-2(3\alpha+4\beta)]$ δηλαδή $\delta_1 \mid \beta$ και
$\delta_1 \mid [3(3\alpha+4\beta)-4(2\alpha+3\beta)]$, δηλαδή $\delta_1 \mid \alpha$.
Επομένως, $\delta_1 \leq \delta_2$, άρα $\delta_1 = \delta_2$.

17. Το (i) είναι προφανές από την Πρόταση 1.3.7.

Για το (ii) ας θεωρήσουμε τους $\delta_1 = (\alpha,\beta)$ και $\delta_2 = \left(\alpha,\, \frac{\beta}{2}\right)$.
Προφανώς $\delta_2 \mid \alpha$, $\delta_2 \mid \beta$ και $\delta_2 \leq \delta_1$.
Επιπλέον, $\delta_1 \mid \alpha$, $\delta_1 \mid \left(2 \cdot \frac{\beta}{2}\right)$ και ο δ_1 είναι περιττός αφού ο α είναι περιττός.
Άρα, από την Πρόταση 1.3.10, πρόκυπτει ότι $\delta_1 \mid \frac{\beta}{2}$ και $\delta_1 \leq \delta_2$.
Επομένως, $\delta_1 = \delta_2$.

18. Αφού τα κλάσματα είναι ανάγωγα, ισχύει ότι $(\alpha,\beta) = (\gamma,\delta) = 1$.
Αν το άθροισμα

$$\frac{\alpha}{\beta} + \frac{\gamma}{\delta} = \frac{\alpha\delta+\beta\gamma}{\beta\delta}$$

είναι ακέραιος, τότε $\beta\delta \mid (\alpha\delta+\beta\gamma)$. Δηλαδή, $\beta \mid (\alpha\delta+\beta\gamma)$ και $\delta \mid (\alpha\delta+\beta\gamma)$, οπότε $\beta \mid \alpha\delta$ και $\delta \mid \beta\gamma$.
Από τη σχέση $(\alpha,\beta) = (\gamma,\delta) = 1$, προκύπτει ότι $\beta \mid \delta$ και $\delta \mid \beta$.
Άρα $\beta = \delta$, άτοπο.

19. Αφού $(\alpha,6) = (\beta,6) = 1$, οι αριθμοί α και β γράφονται στη μορφή $\alpha = 6\varkappa \pm 1$ και $\beta = 6\lambda \pm 1$. Επομένως

$$\alpha^2 = 36\varkappa^2 \pm 12\varkappa + 1 = 12(3\varkappa^2 \pm \varkappa) + 1$$

και

$$\beta^2 = 36\lambda^2 \pm 12\lambda + 1 = 12(3\lambda^2 \pm \varkappa) + 1.$$

Για το (i) έχουμε ότι

$$\alpha^2 - \beta^2 = 12[(3\kappa^2 \pm \kappa) - (3\lambda^2 \pm \lambda)] = \pi o \lambda .12,$$

ενώ για το (ii) ισχύει ότι

$$\alpha^2 + \beta^2 = 12[(3\kappa^2 \pm \kappa) - (3\lambda^2 \pm \lambda)] + 2.$$

Άρα $(\alpha^2 - \beta^2, 12) = 12$ και $(\alpha^2 + \beta^2, 12) = 2$.

20. Έστω x, y τέτοιοι ώστε $(x, y) = 5$. Τότε γράφονται $x = 5\alpha$ και $y = 5\beta$ με $(\alpha, \beta) = 1$, ενώ $x + y = 5(\alpha + \beta)$.
Υπάρχουν άπειροι ακέραιοι α τέτοιοι ώστε $(\alpha,\ 20 - \alpha) = 1$, οπότε $(5\alpha,\ 100 - 5\alpha) = 5$ με $5\alpha + (100 - 5\alpha) = 100$. Άρα υπάρχουν άπειρα ζεύγη ακεραίων $x = 5\alpha$ και $y = 100 - 5\alpha$ τέτοια ώστε $x + y = 100$ και $(x, y) = 5$.

21. Ο αριθμός $N = \nu^5 - \nu$ γράφεται στη μορφή

$$N = (\nu - 1)\nu(\nu + 1)(\nu^2 + 1).$$

Το γινόμενο $(\nu - 1)\nu(\nu + 1)$ διαιρείται τέλεια με τον αριθμό 6, ενώ ο αριθμός 5 διαιρεί τέλεια τον αριθμό N. Αφού (5,6)=1, προκύπτει ότι $30 \mid N$.

22. Ο αριθμός $N = \nu^7 - \nu$ γράφεται στη μορφή

$$N = \nu(\nu - 1)(\nu + 1)(\nu^2 + \nu + 1)(\nu^2 - \nu + 1).$$

Γνωρίζουμε ότι $6 \mid \nu(\nu - 1)(\nu + 1)$, δηλαδή ότι $6 \mid N$. Ελέγχουμε περιπτώσεις ανάλογα με το υπόλοιπο της διαίρεσης του ν δια 7:

(i) Αν $\nu = 7\kappa$ ή $\nu = 7\kappa + 1$ ή $\nu = 7\kappa + 6$, τότε προφανώς $7 \mid \nu(\nu - 1)(\nu + 1)$, οπότε $7 \mid N$.

(ii) Αν $\nu = 7\kappa + 2$ τότε $\nu^2 + \nu + 1 = 7(7\kappa^2 + 5\kappa + 1)$ και $7 \mid N$.

Όμοια ελέγχουμε και τις υπόλοιπες περιπτώσεις.

23. Έστω το γινόμενο $N = \nu(\nu + 1)(\nu + 2)(\nu + 3)$. Προφανώς ένας από τους παράγοντες θα είναι πολλαπλάσιο του 3, άρα $3 \mid N$.

Διακρίνουμε περιπτώσεις ως προς το υπόλοιπο της διαίρεσης του ν δια 4.

(i) Αν $\nu = 4\kappa$, τότε $4 \mid \nu$ και $2 \mid (\nu + 2)$.

(ii) Αν $\nu = 4\kappa + 1$, τότε $4 \mid (\nu + 3)$ και $2 \mid (\nu + 1)$.

(iii) Αν $\nu = 4\kappa + 2$, τότε $4 \mid (\nu + 2)$ και $2 \mid \nu$.

(iv) Αν $\nu = 4\kappa + 3$, τότε $4 \mid (\nu + 1)$ και $2 \mid (\nu + 3)$.

Άρα σε όλες τις περιπτώσεις $8 \mid N$, $3 \mid N$ και αφού (8,3)=1 έχουμε ότι $24 \mid N$.

24. Ο αριθμός $N = 1492^\nu - 1770^\nu - 1863^\nu + 2141^\nu$ γράφεται

$$N = (2141^\nu - 1863^\nu) - (1770^\nu - 1492^\nu) \text{ ή}$$

$$N = (2141 - 1863)(2141^{\nu-1} + \ldots + 1863^{\nu-1})$$

$$-(1770 - 1492)(1770^{\nu-1} + \ldots + 1492^{\nu-1}) \text{ ή}$$

$$N = 278(2141^{\nu-1} + \ldots + 1863^{\nu-1} - 1770^{\nu-1} - \ldots - 1492\nu - 1).$$

Επίσης γράφεται

$$N = (2141^\nu - 1770^\nu) - (1863^\nu - 1492^\nu) \text{ ή}$$

$$N = (2141 - 1770)(2141^{\nu-1} + \ldots + 1770\nu - 1)$$

$$-(1863 - 1492)(1863^{\nu-1} + \ldots 1492^{\nu-1}) \text{ ή}$$

$$N = 371(2141^{\nu-1} + \ldots + 1770^{\nu-1} - 1863\nu - 1 - \ldots - 1492^{\nu-1}).$$

Δηλαδή ο αριθμός N είναι πολλαπλάσιο των $278 = 2 \cdot 139$ και $371 = 7 \cdot 53$, οι οποίοι είναι πρώτοι μεταξύ τους. Άρα $(2 \cdot 139 \cdot 7) \mid N$ ή $1946 \mid N$.

25. Είναι $\alpha^2(\alpha^2 - 1)(\alpha^2 - 4) = (\alpha - 2)(\alpha - 1)\alpha(\alpha + 1)(\alpha + 2)\alpha$.
Σε 5 διαδοχικούς αριθμούς υπάρχουν τουλάχιστον δύο πολλαπλάσια του 3, δύο πολλαπλάσια του 2, από τα οποία ένα τουλάχιστον είναι πολλπλάσιο του 4 και ένα πολλαπλάσιο του 5.

Έτσι, ο αριθμός $\alpha^2(\alpha^2-1)(\alpha^2-4)$ διαιρείται με τους αριθμούς 9,8,5 και επειδή αυτοί οι αριθμοί είναι πρώτοι μεταξύ τους ανά δύο, θα διαιρείται και με τον $9 \cdot 8 \cdot 5 = 360$.

26. Παρατηρούμε ότι:

$$3(14\nu + 3) - 2(21\nu + 4) = 1,$$

οπότε οι αριθμοί $14\nu + 3$ και $21\nu + 4$ είναι πρώτοι μεταξύ τους.

27. Αφού α, γ περιττοί, από τη σχέση $\alpha^2 + \beta^2 = \gamma^2$ έχουμε ότι ο β είναι άρτιος. Έστω $\delta = (\beta + \gamma\,,\, \gamma - \beta)$.
Τότε ο δ διαιρεί τους αριθμούς

$$\begin{aligned} & (\beta + \gamma) + (\gamma - \beta) = 2\gamma \\ \text{και} \quad & (\beta + \gamma) - (\gamma - \beta) = 2\beta. \end{aligned}$$

Όμως ο δ είναι περιττός, αφού οι $\beta + \gamma$, $\gamma - \beta$ είναι περιττοί άρα ο δ διαιρεί τους γ και β επίσης. Αφού όμως $(\beta, \gamma) = 1$, έχουμε $\delta = 1$.
Έτσι επειδή $(\beta + \gamma)(\beta - \gamma) = \alpha^2$ και $\delta = 1$, συμπεραίνουμε ότι οι αριθμοί $\beta + \gamma$, $\gamma - \beta$ είναι επίσης τέλεια τετράγωνα.

Λύσεις Ασκήσεων §1.4

Α' Ομάδα

1. Όμοια με Εφαρμογή 1 §1.4.

2. Όμοια με Εφαρμογή 1 §1.4.

3. Όμοια με Εφαρμογή 1 §1.4.

4. Όμοια με την Εφαρμογή 2 §1.4.

5. (i) Αν x, y είναι δύο θετικοί ακέραιοι, τότε $x \geq 1$ και $y \geq 1$. Επομένως, $7x + 15y \geq 22$ και η εξίσωση $7x + 15y = -10$ αποκλείεται να έχει λύση για $x, y > 0$.

   (ii) Παρατηρούμε ότι (3,15)=3 με $3 \nmid 16$, άρα η εξίσωση $3x + 15y = 16$ δεν έχει λύση, από το Θεώρημα 1.4.1.

   (iii) Όμοια με το (i).

6. Θέλουμε $\frac{9-7x}{4} = πολ.3$, δηλαδή να υπάρχει ακέραιος y τέτοιος ώστε

$$\frac{9-7x}{4} = 3y \text{ ή}$$

$$7x + 12y = 9.$$

   Η παραπάνω γραμμική Διοφαντική εξίσωση έχει πάντα λύση, διότι (7,12)=1 και $1 \mid 9$. Επίσης, παρατηρούμε ότι

$$7(-5) + 12 \cdot 3 = 1$$

   και πολλαπλασιάζοντας με 9 έχουμε ότι

$$7(-45) + 12 \cdot 27 = 9.$$

   Δηλαδή, μία λύση της εξίσωσης είναι $x_0 = -45$, $y_0 = 27$. Η Διοφαντική εξίσωση έχει άπειρες λύσεις της μορφής

$$\begin{aligned} x &= -45 + 12t \\ y &= 27 - 7t, \end{aligned}$$

   για κάθε ακέραιο t. Άρα το πηλίκο $\frac{9-7x}{4}$ είναι πολλαπλάσιο του 3 για κάθε ακέραιο της μορφής $x = -45 + 12t$, όπου $t \in \mathbf{Z}$.

7. Από τον αλγόριθμο του Ευκλείδη γνωρίζουμε ότι υπάρχει τουλάχιστον ένα ζευγάρι (κ, λ) ώστε $\delta = \kappa\alpha + \lambda\beta$.
Αλλά για κάθε μ έχουμε

$$\kappa'\alpha + \lambda'\beta = (\kappa - \mu\beta)\alpha + (\lambda + \mu\alpha)\beta = \kappa\alpha + \lambda\beta = \delta$$

όπου $\kappa' = \kappa - \mu\beta$ και $\lambda' = \lambda + \mu\alpha$. Οπότε οι κ, λ δεν είναι μοναδικοί.
Επιπλέον, το πλήθος των ζευγών (κ, λ) είναι άπειρο.

Β' Ομάδα

8. Αν x είναι το πλήθος των ενήλικων θεατών και y είναι το πλήθος των παιδιών, τότε έχουμε τη γραμμική Διοφαντική εξίσωση

$$1800x + 750y = 90000$$

την οποία και λύνουμε όμοια με την Εφ. 1 § 1.4.

9. Έστω τα κλάσματα $x/5$ και $y/7$ τέτοια ώστε

$$\frac{x}{5} + \frac{y}{7} = \frac{26}{35}$$

ή

$$\frac{7x + 5y}{5} = \frac{26}{5}.$$

Έτσι έχουμε τη γραμμική Διοφαντική εξίσωση

$$7x + 5y = 26$$

η οποία έχει λύση διότι (7,5)=1 με $1 \mid 26$. Παρατηρούμε ότι

$$7(-2) + 5 \cdot 3 = 1$$

ή

$$7(-52) + 5 \cdot 78 = 26$$

και μια λύση της Διοφαντικής εξίσωσης είναι $x_0 = -52$ και $y_0 = 78$. Από το Θεώρημα 1.4.2 έχει άπειρες λύσεις της μορφής

$$\begin{aligned} x &= -52 + 5t \\ y &= 78 - 7t \end{aligned}$$

για κάθε ακέραιο t. Άρα τα ζητούμενα χλάσματα είναι τα

$$\frac{-52 + 5t}{5} \text{ και } \frac{78 - 7t}{7}$$

όπου $t \in \mathbf{Z}$.

10. Αφού οι ακέραιοι x και y είναι πολλαπλάσια του 5, υπάρχουν ακέραιοι ω και z τέτοιοι ώστε $x = 5\omega$ και $y = 5z$. Επομένως, έχουμε τη γραμμική Διοφαντική εξίσωση

$$3\omega + 4z = 10$$

η οποία λύση διότι (3,4)=1 με $1 \mid 10$.
Παρατηρούμε ότι $1 = 3(-1) + 4 \cdot 1$ και πολλαπλασιάζοντας με 10 έχουμε ότι $3(-10) + 4 \cdot 10 = 10$, δηλαδή μία λύση είναι $\omega_0 = -10$, $z_0 = 10$.
Η γραμμική Διοφαντική εξίσωση $3\omega + 4z = 10$ έχει άπειρες λύσεις της μορφής

$$\omega = -10 + 4t$$

$$z = 10 - 3t,$$

όπου $t \in \mathbf{Z}$. Οπότε, η εξίσωση $3x + 4y = 50$ με τους x, y να είναι πολλαπλάσια του 5 έχει άπειρες λύσεις της μορφής

$$x = -50 + 20t$$

$$y = 50 - 15t,$$

όπου $t \in \mathbf{Z}$.

11. Η εξίσωση $(3x + 2y - 4)^2 = (2x + y - 5)^2$ γράφεται

$$(3x + 2y - 4)^2 - (2x + y - 5)^2 = 0 \text{ ή}$$

$$(x+y-1)(5x+3y-9)=0$$

Επομένως, έχουμε δύο γραμμικές Διοφαντικές εξισώσεις

$$x+y=-1$$

και

$$5x+3y=9$$

οι οποίες έχουν και οι δύο άπειρες λύσεις διότι $(1,1) \mid (-1)$ και $(5,3) \mid 9$.
Υπολογίζουμε τις λύσεις τους, όπως στην Εφ. 1 § 1.4 και η ένωση αυτών των λύσεων είναι οι λύσεις της εξίσωσης $(3x+2y-4)^2 = (22x+y-5)^2$.

12. Η εξίσωση $(\sqrt{\lambda}-1)x^2+2\sqrt{\mu}x-3(\sqrt{\lambda}+1)=0$ έχει μια διπλή ρίζα αν και μόνο αν

$$\Delta = 4\mu+12(\lambda-1)=0,$$

δηλαδή αν

$$\mu+3\lambda=3.$$

Έχουμε μια γραμμική Διοφαντική εξίσωση, η οποία έχει λύση διότι (1,3)=1 και $1 \mid 3$. Παρατηρούμε ότι

$$1\cdot 0+3\cdot 1=3$$

και προφανώς μια λύση της Διοφαντικής εξίσωσης είναι $\mu_0=0$, $\lambda_0=1$. Επομένως, έχει άπειρες λύσεις της μορφής

$$\begin{aligned}\mu &= 3t\\ \lambda &= 3-t,\end{aligned}$$

για κάθε ακέραιο t.

13. Η εξίσωση $y^2-6x^2+xy-y+17x-12=0$ γράφεται ως τριώνυμο του y :

$$y^2+(x-1)y+(-6x^2+17x-12)=0$$

με διακρίνουσα $\Delta=(x-1)^2-4(-6x^2+17x-12)=(5x-7)^2$ και ρίζες

$$y=\frac{-x+1+5x-7}{2}=2x-3$$

και

$$y = \frac{-x + 1 - 5x + 7}{2} = -3x + 4.$$

Η αρχική εξίσωση γράφεται

$$(y - 2x + 3)(y + 3x - 4) = 0,$$

οπότε πρέπει να ισχύει $y - 2x = -3$ ή $y + 3x = 4$. Λύνουμε αυτές τις δύο γραμμικές Διοφαντικές εξισώσεις και η ένωση των λύσεών τους είναι οι λύσεις της εξίσωσης $y^2 - 6x^2 + xy - y + 17x - 12 = 0$.

14. Η γραμμική Διοφαντική εξίσωση $5x + 7y = \gamma$ έχει πάντα λύσεις διότι (5,7)=1 με $1 \mid \gamma$. Παρατηρούμε ότι

$$5 \cdot 3 + 7(-2) = 1$$

και πολλαπλασιάζοντας με γ έχουμε ότι

$$5(3\gamma) + 7(-2\gamma) = \gamma.$$

Δηλαδή μία λύση της Διοφαντικής εξίσωσης είναι $x_0 = 3\gamma$, $y_0 = -2\gamma$. Έχουμε λοιπόν άπειρες λύσεις της μορφής

$$\begin{aligned} x &= 3\gamma + 7t \\ y &= -2\gamma - 5t, \end{aligned}$$

με $t \in \mathbf{Z}$. Οι λύσεις αυτές είναι θετικές αν και μόνο αν

$$3\gamma + 7t > 0 \text{ ή } t > -\frac{3\gamma}{7}$$

και

$$-2\gamma - 5t > 0 \text{ ή } t < -\frac{2\gamma}{5}.$$

Επομένως, έχουμε 9 θετικές λύσεις αν

$$9 < -\tfrac{2\gamma}{5} - \left(-\tfrac{3\gamma}{7}\right) < 10$$

$$\text{ή} \qquad 9 < \tfrac{15\gamma - 14\gamma}{35} < 10$$

$$\text{ή} \qquad 315 < \gamma < 350.$$

Όμως παρατηρούμε ότι και στην περίπτωση $\gamma = 350$ έχουμε 9 θετικές λύσεις για $t = -149, -148, \ldots, -141$. Άρα ο μεγαλύτερος ακέραιος γ που μας δίνει 9 ακριβώς θετικές λύσεις είναι ο $\gamma = 350$.

15. Αν έχουμε x κέρματα των 5 δραχμών και y κέρματα των 10 δραχμών, τότε θα έχουμε και $z = 24 - x - y$ κέρματα των 20 δραχμών.
Με τον τρόπο αυτό προκύπτει η Διοφαντική εξίσωση

$$\begin{aligned} 5x + 10y + 20(24 - x - y) &= 200 \text{ ή} \\ -15x - 10y + 480 &= 200 \text{ ή} \\ 15x + 10y &= 280. \end{aligned}$$

Αφού (15,10)=5 με $5 \mid 280$, από το Θεώρημα 1.4.1, η γραμμική Διοφαντική εξίσωση έχει λύση. Παρατηρούμε ότι

$$15 \cdot 1 + 10(-1) = 5$$

και πολλαπλασιάζοντας με τον αριθμό 56 παίρνουμε ότι

$$15 \cdot 56 + 10(-56) = 280,$$

δηλαδή μια λύση είναι $x_0 = 56$, $y_0 = -56$.
Από το Θεώρημα 1.4.2 η Διοφαντική εξίσωση έχει άπειρες λύσεις της μορφής

$$x = 56 + \left(\frac{10}{5}\right) t = 56 + 2t$$

$$y = -56 - \left(\frac{15}{5}\right) t = -56 - 3t,$$

όπου $t \in \mathbf{Z}$.
Όμως, οι αριθμοί x και y ικανοποιούν τις σχέσεις $0 \leq x \leq 24$, $0 \leq y \leq 24$ και $0 \leq x + y \leq 24$. Επομένως,

$$\begin{aligned} & 0 \leq 56 + 2t \leq 24, \quad 0 \leq -56 + 3t \leq 24 \quad \text{και} \quad 0 \leq -t \leq 24 \\ \text{ή} \quad & -28 \leq t \leq -16, \qquad -\tfrac{80}{3} \leq t \leq -\tfrac{56}{3} \qquad \text{και} \quad -24 \leq t \leq 0. \end{aligned}$$

Οι τρεις ανισώσεις συναληθεύονται για $t = -24, \ldots, -19$ και έχουμε 6 δυνατούς συνδυασμούς:

$$\begin{aligned} x = 8 \quad y = 16 \quad z = 0, \\ x = 10 \quad y = 13 \quad z = 1, \\ x = 12 \quad y = 10 \quad z = 2, \\ x = 14 \quad y = 7 \quad z = 3, \\ x = 16 \quad y = 4 \quad z = 4, \\ x = 18 \quad y = 1 \quad z = 5. \end{aligned}$$

Λύσεις Ασκήσεων § 1.5

Α' Ομάδα

1. Απλή εφαρμογή του ορισμού του Ε.Κ.Π.

2. Όμοια με Εφαρμογή 2 §1.5.

3. (i) Προφανώς $(\nu, \nu+1) = (\nu, 1) = 1$ και από την Πρόταση 1.5.4 προκύπτει ότι $[\nu, \nu+1] = \nu(\nu+1)$.

   (ii) Προφανώς $(2\nu-1, 2\nu+1) = (2\nu-1, 2) = 1$ και από την Πρόταση 1.5.4 προκύπτει ότι $[2\nu-1, 2\nu+1] = (2\nu-1)(2\nu+1)$.

4. Οι α, β γράφονται $\alpha = 10\gamma$ και $\beta = 10\delta$. Επιπλέον

$$\begin{aligned} \alpha\beta &= (\alpha,\beta)[\alpha,\beta] \text{ ή} \\ 100\gamma\delta &= 1000 \text{ ή} \\ \gamma\delta &= 10, \end{aligned}$$

   με $0 < \gamma \leq \delta$. Έχουμε λοιπόν δύο περιπτώσεις:

$$\begin{aligned} \gamma = 1, \quad \delta = 10 \quad \text{και} \quad \alpha = 10, \quad \beta = 100 \text{ ή} \\ \gamma = 2, \quad \delta = 5 \quad \text{και} \quad \alpha = 20, \quad \beta = 50. \end{aligned}$$

5. Θέλουμε τον ελάχιστο φυσικό N, τέτοιον ώστε

$$2 \mid (N-1), 3 \mid (N-2), \ldots, 10 \mid (N-9)$$

   ή ισοδύναμα

$$2 \mid (N+1), 3 \mid (N+1), \ldots, 10 \mid (N+1),$$

   δηλαδή ο N+1 είναι το ελάχιστο κοινό πολλαπλάσιο των αριθμών $2, 3, 4 = 2^2, 5, 6 = 2 \cdot 3, 7, 8 = 2^3, 9 = 3^2, 10 = 2 \cdot 5$.
   Άρα $N + 1 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$, οπότε N=2519.

Λύσεις Ασκήσεων §1.6

Α' Ομάδα

1. Προφανής από τους ορισμούς των πρώτων αριθμών και του Μ.Κ.Δ.

2. Προφανής από το Θεώρημα 1.3.9.

3. Όμοια με την προηγούμενη άσκηση, χρησιμοποιώντας το Θεώρημα 1.3.9.

4. Κάθε φυσικός της μορφής $\nu = 3\kappa + 1$ γράφεται στις μορφές :

$$\nu = 6\lambda + 1 \ \ \acute{\eta} \ \ \nu = 6\lambda + 4.$$

   Όμως ο αριθμός $6\lambda + 4$ είναι άρτιος και μεγαλύτερος του 3, άρα αποκλείεται να είναι πρώτος.

5. Όμοια με την απόδειξη της Πρότασης 1.6.2.

6. Έχουμε:

$$\begin{aligned} 1234 &= 2 \cdot 617 \\ 10140 &= 2^2 \cdot 3 \cdot 5 \cdot 13^2 \\ \kappa\alpha\iota \quad 36000 &= 2^5 \cdot 3^2 \cdot 5^3. \end{aligned}$$

7. Γράφουμε τους 5247000 και 189280 στην κανονική τους μορφή

$$\begin{aligned} 5247000 &= 2^3 \cdot 3^2 \cdot 5^3 \cdot 11 \cdot 53 \\ \kappa\alpha\iota \quad 189280 &= 2^5 \cdot 5 \cdot 7 \cdot 13^2. \end{aligned}$$

   Άρα $(5247000, 189280) = 2^3 \cdot 5 = 40$.

8. Προφανής, αφού κάθε κοινός διαιρέτης των α, β έχει παράγοντες της μορφής $p_i^{\gamma_i}$ με $\gamma_i \leq \min\{\alpha, \beta\}$, ενώ κάθε κοινό πολλαπλάσιο των α, β έχει παράγοντες της μορφής $p_i^{\delta_i}$ με $\delta_i \geq \max\{\alpha, \beta\}$.

9. Ένας πρώτος αριθμός $p > 3$ γράφεται ως $p = 3\kappa + 1$ ή $p = 3\kappa + 2$. Αν $p = 3\kappa + 2$, τότε αποκλείεται ο κ να είναι άρτιος, αφού θα ήταν και ο p άρτιος.
   Άρα ο κ γράφεται ως $\kappa = 2\nu + 1$ και $p = 6\nu + 5$.

10. Κάθε άρτιος $\nu > 11$ γράφεται στη μορφή $\nu = 4 + (\nu - 4)$, όπου οι αριθμοί 4 και $\nu - 4$ είναι σύνθετοι, ως άρτιοι.
Κάθε περιττός $\nu > 11$ γράφεται στη μορφή $\nu = 9 + (\nu - 9)$, όπου οι αριθμοί $9 = 3^2$ και $\nu - 9$ (ως άρτιος) είναι σύνθετοι.

11. Για να είναι οι αριθμοί p και $p+4$ πρώτοι, πρέπει $p = 3\kappa + 1$ οπότε $p + 4 = 3\kappa + 5$. Έτσι ο αριθμός $N = 3p + 6$ γράφεται

$$\begin{aligned} N &= (p+1) + (p+2) + (p+3) \\ &= 3\kappa + 2 + 3\kappa + 3 + 3\kappa + 4 \\ &= 9\kappa + 9 = 9(\kappa + 1). \end{aligned}$$

12. Γράφουμε τους α και β ως γινόμενο πρώτων παραγόντων

$$\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\nu^{\alpha_\nu}$$

$$\beta = p_1^{\beta_1} p_2^{\beta_2} \dots p_\nu^{\beta_\nu}$$

όπου όλοι οι εκθέτες είναι μη αρνητικοί. Οι αριθμοί α^κ και β^κ γράφονται

$$\alpha^\kappa = p_1^{\kappa\alpha_1} p_2^{\kappa\alpha_2} \dots p_\nu^{\kappa\alpha_\nu}$$

$$\beta^\kappa = p_1^{\kappa\beta_1} p_2^{\kappa\beta_2} \dots p_\nu^{\kappa\beta_\nu}$$

και αφού $\alpha^\kappa \mid \beta^\kappa$, είναι προφανές ότι $\kappa\alpha_j < \kappa\beta_j$, για κάθε $j = 1, 2, \dots, \nu$. Άρα $\alpha_j < \beta_j$, για κάθε $j = 1, 2, \dots, \nu$ και $\alpha \mid \beta$.

13. Λύνουμε όμοια με προηγούμενη άσκηση, γράφοντας α και β ως γινόμενα πρώτων παραγόντων και συγκρίνοντας τους αντίστοιχους εκθέτες.

14. Αν ο αριθμός ν είναι άρτιος, τότε προφανώς και ο $N = \nu^2 + 2^\nu$ είναι άρτιος.
Αν ο αριθμός ν είναι περιττός, τότε θα είναι της μορφής $\nu = 6\kappa + 1$ ή $\nu = 6\kappa + 5$. Για $\nu = 6\kappa + 1$, ο αριθμός

$$\begin{aligned} N = \nu^2 + 2^\nu &= (6\kappa + 1)^2 + 2^{6\kappa+1} \\ &= 36\kappa^2 + 12\kappa + 1 + 2(63 + 1)^\kappa \\ &= 36\kappa^2 + 12\kappa + 2 \cdot 63(63^{\kappa-1} + \dots + \kappa) + 3 \end{aligned}$$

είναι πολλαπλάσιο του αριθμού 3.
Για $\nu = 6\kappa + 5$, εργαζόμαστε ανάλογα.

15. Όμοια με προηγούμενη άσκηση.

16. Προφανώς ο αριθμός 50! έχει παράγοντες όλους τους πρώτους 2,3,5,...,47,
Έστω ότι $p \mid 50!$ με p πρώτο, $p > 47$ οπότε $p \geq 53$. Τότε, επειδή $50! = 2 \cdot 3 \cdot 4 \cdot 5 \ldots 50$ και p πρώτος πρέπει
$p \mid 2$ ή $p \mid 3$ ή $p \mid 4 \ldots$ ή $p \mid 50$ άτοπο, αφού $p \geq 53$.
Άρα οι πρώτοι παράγοντες του 50! είναι οι 2, 3, 4, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

17. Γράφουμε τον αριθμό 945 στην κανονική του μορφή

$$945 = 3^3 \cdot 5 \cdot 7.$$

Ο ελάχιστος φυσικός ν που απαιτείται ώστε ο αριθμός 945ν να είναι τέλειο τετράγωνο ακεραίου, είναι ο

$$\nu = 3 \cdot 5 \cdot 7 = 105.$$

Πράγματι, $945\nu = 3^4 \cdot 5^2 \cdot 7^2 = (3^2 \cdot 5 \cdot 7)^2 = 315^2$.

Β' Ομάδα

18. Ένας από τους τρεις διαδοχικούς αριθμούς

$$2^\nu - 1,\ 2^\nu,\ 2^\nu + 1$$

διαιρείται με το 3. Αλλά ο αριθμός 2^ν δεν διαιρείται ποτέ με το 3.

19. Επειδή $\alpha(\alpha+\beta+\gamma+\delta) = (\alpha+\gamma)(\alpha+\delta)$, αν ο $\alpha+\beta+\gamma+\delta$ ήταν πρώτος, θα έπρεπε να διαιρεί έναν από τους $\alpha+\gamma$, $\alpha+\delta$, αδύνατο αφού ο $\alpha+\beta+\gamma+\delta$ είναι μεγαλύτερός τους.
Έτσι ο $\alpha+\beta+\gamma+\delta$ είναι σύνθετος.

20. Έστω ο ένας πρώτος αριθμός της μορφής

$$p = x^3 + 1 = (x+1)(x^2 - x + 1),$$

όπου $x \geq 1$. Πρέπει ένας από τους παράγοντες $x+1$ ή x^2-x+1 να ισούται με τη μονάδα. Όμως, $x+1 \geq 2$, άρα πρέπει $x^2-x+1 = 1$. Δηλαδή, $x = 0$ ή $x = 1$. Επομένως, $x = 1$ και $p = 1^3 + 1 = 2$.

21. Αφού $(\alpha, p^2) = p$ και $(\beta, p^4) = p^2$, έχουμε ότι $p \mid \alpha$ με $p^2 \nmid \alpha$ και $p^2 \mid \beta$ με $p^3 \nmid \beta$. Επομένως,

$$p^3 \mid \alpha\beta \text{ και } p^4 \nmid \alpha\beta, \text{ άρα } (\alpha\beta, p^5) = p^3,$$

$$p \mid (\alpha + \beta) \text{ και } p^2 \nmid (\alpha + \beta), \text{ άρα } (\alpha + \beta, p^2) = p,$$

$$p \mid (\alpha - \beta) \text{ και } p^2 \nmid (\alpha - \beta), \text{ άρα } (\alpha - \beta, p^5) = p,$$

$$p^2 \mid (p\alpha - \beta) \text{ και } p^3 \nmid (p\alpha - \beta), \text{ άρα } (p\alpha - \beta, p^5) = p^2,$$

22. Γνωρίζουμε ότι στο γινόμενο
$p(p+1)(p+2)$ υπάρχουν ένας άρτιος παράγοντας κι ένας παράγοντας που είναι πολλαπλάσιο του 3.
Όμως οι περιττοί πρώτοι p και $p+2$ δεν είναι ούτε άρτιοι, ούτε πολλαπλάσια του 3. Άρα $2 \mid (p+1)$ και $3 \mid (p+1)$, δηλαδή $6 \mid (p+1)$.

23. Έστω ο πρώτος αριθμός

$$\begin{aligned} p &= \alpha^4 - \beta^4 \\ &= (\alpha^2 - \beta^2)(\alpha^2 + \beta^2) \\ &= (\alpha - \beta)(\alpha + \beta)(\alpha^2 + \beta^2). \end{aligned}$$

Πρέπει $\alpha - \beta = \alpha + \beta = 1$, άρα $\alpha = 1$ και $\beta = 0$. Επομένως, δεν υπάρχει πρώτος αριθμός της μορφής $p = \alpha^4 - \beta^4$.

24. Έστω $\nu = \kappa^2$ και $\nu + 1 = \lambda^2$ δύο διαδοχικοί θετικοί ακέραιοι που είναι τέλεια τετράγωνα των φυσικών κ και λ. Τότε έχουμε

$$\lambda^2 - \kappa^2 = (\nu + 1) - \nu = 1 \text{ ή}$$

$$(\lambda - \kappa)(\lambda + \kappa) = 1.$$

Άρα $\lambda - \kappa = \lambda + \kappa = 1$, οπότε $\kappa = 0$ και $\lambda = 1$. Δηλαδή καταλήγουμε ότι $\nu = 0$, άτοπο.

25. Έστω $\nu = p + q = 154\kappa + 9$, όπου p, q πρώτοι.
Επειδή ο ν είναι περιττός, ένας από τους p, q θα είναι άρτιος, δηλαδή ο αριθμός 2.
Άρα $p = 154\kappa + 7 = 7(22\kappa + 1)$ δηλαδή $\kappa = 0$, αφού ο p είναι πρώτος. Έτσι έχουμε $\nu = 7 + 2 = 9$.

Όμοια, αν υποθέσουμε ότι $\nu = p - q = 154x + 9$ παίρνουμε $p = 154x + 11 = 11(14x + 1)$, οπότε $x = 0$ και έτσι $p = 11$ άρα $\nu = 11 - 2 = 9$.
Έτσι ο ζητούμενος αριθμός είναι ο 9.

26. Ένας πρώτος αριθμός $p > 3$ είναι της μορφής $p = 3x + 1$ ή $p = 3x + 2$.
Αν $p = 3x+1$, τότε $p^2 = (3x+1)^2 = 9x^2+6x+1 = 3x(3x+2)+1$, όπου οι αριθμοί x και $3x + 2$ είναι άρτιοι, άρα $12 \mid [3x(3x + 2)]$.
Αν $p = 3x + 2$, τότε ο αριθμός x είναι περιττός και ο p γράφεται $p = 6\lambda + 5$, άρα έχουμε ότι :
$p^2 = (6\lambda + 5)^2 = 36\lambda^2 + 60\lambda + 25 = 12(3\lambda^2 + 5\lambda + 2) + 1$.
Άρα, πάντα ο p είναι της μορφής $p^2 = 12\nu + 1$.

27. Έστω $\nu = 2x$, οπότε ο αριθμός N γράφεται

$$N = \overbrace{111\ldots1}^{\nu-\psi\eta\phi\acute{\iota}\alpha} = \frac{\overbrace{999\ldots9}^{\nu-\psi\eta\phi\acute{\iota}\alpha}}{9} \text{ ή}$$

$$N = \frac{10^{\nu}-1}{9} = \frac{(10^2)^x-1}{9} \text{ ή}$$

$$N = \frac{(10^2-1)(10^{2(x-1)}+10^{2(x-2)}+\ldots+10^2+1)}{9} \text{ ή}$$

$$N = 11(10^{2(x-1)} + 10^{2(x-2)} + \ldots + 10^2 + 1).$$

Προφανώς ο N είναι σύνθετος.

28. Γενικότερα θα αποδείξουμε ότι αυτό ισχύει για τον αριθμό $N = 111\ldots1$ γραμμένο σε οποιοδήποτε σύστημα αρίθμησης με βάση τον $\alpha \geq 2$. (Στην περίπτωσή μας $\alpha = 10$.)
Αν ο ν είναι σύνθετος, δηλαδή $\nu = x\lambda$ τότε

$$N = \underbrace{(111\ldots1)_{\alpha}}_{\nu} = \frac{\alpha^{\nu}-1}{\alpha-1} \text{ ή}$$

$$N = \frac{\alpha^{x\lambda}-1}{\alpha-1} = \frac{\alpha^{x}-1}{\alpha-1}\left(\alpha^{x(\lambda-1)} + \alpha^{x(\lambda-2)} + \ldots + 1\right) \text{ ή}$$

$$N = (\alpha^{x-1} + \alpha^{x-2} + \ldots + 1)\left(\alpha^{x(\lambda-1)} + \alpha^{x(\lambda-1)} + \ldots + 1\right)$$

δηλαδή ο αριθμός N είναι σύνθετος.

29. Αφού $p \mid \alpha\beta$, γνωρίζουμε ότι ο πρώτος p θα είναι παράγοντας του α ή του β. Ας υποθέσουμε χωρίς βλάβη της γενικότητας ότι $p \mid \alpha$. Επιπλέον, $p \mid (\alpha+\beta)$, άρα $p \mid [(\alpha+\beta)-\alpha]$ δηλαδή $p \mid \beta$. Επομένως, καταλήγουμε ότι $p \mid (\alpha, \beta)$.

30. Οι φυσικοί α και β είναι πρώτοι μεταξύ τους, δηλαδή $(\alpha, \beta) = 1$. Ας υποθέσουμε ότι $\delta = (\alpha+\beta, \alpha-\beta) > 1$. Τότε ο αριθμός δ έχει τουλάχιστον έναν πρώτο διαιρέτη p, ο οποίος θα διαιρεί το άθροισμα $\alpha+\beta$ και το γινόμενο $\alpha \cdot \beta$.
Από την προηγούμενη άσκηση, έχουμε ότι $p \mid (\alpha, \beta)$, άρα $p \leq 1$, άτοπο.

31. Έστω $\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ η κανονική γραφή του α. Τότε η κανονική μορφή του α^ν είναι

$$\alpha^\nu = p_1^{\nu\alpha_1} p_2^{\nu\alpha_2} \ldots p_\kappa^{\nu\alpha_\kappa}$$

και αφού $p \mid \alpha^\nu$ προκύπτει ότι ο p είναι ένας πρώτος παράγοντας του α^ν. Επομένως, ο p είναι πρώτος παράγοντας του α και $p \mid \alpha$.

32. Έστω δύο θετικοί ακέραιοι $\nu = \kappa^2$ και $\nu + p = \lambda^2$, όπου ο p είναι πρώτος και οι κ, λ φυσικοί αριθμοί.
Έχουμε $\lambda^2 - \kappa^2 = (\nu+p) - \nu = p$ ή $(\lambda-\kappa)(\lambda+\kappa) = p$, άρα $\lambda - \kappa = 1$ και $\lambda + \kappa = p$.
Αν ο p είναι περιττός, τότε $\lambda = \frac{p+1}{2}$ και $\kappa = \frac{p-1}{2}$.
Αν $p = 2$, $2\lambda = 3$, άτοπο.
Επομένως, για κάθε περιττό p οι αριθμοί $\nu = \left(\frac{p-1}{2}\right)^2$ και $\nu + p = \left(\frac{p+1}{2}\right)^2$ είναι τέλεια τετράγωνα και διαφέρουν κατά p.

33. Αν ο αριθμός $\kappa^\nu + 1$ είναι πρώτος μεγαλύτερος του 2, τότε ο κ^ν πρέπει να είναι άρτιος, άρα και ο κ είναι άρτιος.
Αν υποθέσουμε ότι ο ν έχει έναν πρώτο παράγοντα $p \geq 3$, τότε γράφεται $\nu = p \cdot \mu$ και ο αριθμός

$$\begin{aligned} \kappa^\nu + 1 &= (\kappa^\mu)^p + 1 \\ &= (\kappa^\mu + 1)[(\kappa^\mu)^{p-1} - (\kappa^\mu)^{p-2} \ldots - \kappa^\mu + 1] \end{aligned}$$

είναι σύνθετος, άτοπο. Επομένως, ο ν είναι μία δύναμη του 2.

34. Αν $\delta = 1$, τότε προφανώς $p = q = 1$.
Αν $\delta > 1$ και $\delta = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa}$ είναι η κανονική μορφή του δ, τοτε κάθε πρώτος παράγοντας του δ είναι παράγοντας του μ ή του ν. Επιπλέον, οι φυσικοί μ και ν δεν έχουν κοινό πρώτο παράγοντα, διότι $(\mu, \nu)=1$.
Επομένως, ο δ γράφεται $\delta = p \cdot q$, όπου p είναι το γινόμενο όλων των κοινών πρώτων παραγόντων των δ και μ , ενώ q είναι το γινόμενο όλων των κοινών πρώτων παραγόντων των δ και ν.

35. Έστω ένας πρώτος αριθμός $p \geq 5$. Τότε γράφεται ως $p = 3\nu + 1$ ή $p = 6\nu + 1$.

i) Αν $p = 3\nu + 1$, τότε ο αριθμός $p^2 + 2 = (3\nu + 1)^2 = 9\nu^2 + 6\nu + 3 = 3(3\nu^2 + 2\nu + 1)$ είναι σύνθετος.

ii) Αν $p = 6\nu + 1$, τότε ο αριθμός $p^2 + 2 = (6\nu + 1)^2 + 2 = 36\nu^2 + 12\nu + 3 = 3(12\nu^2 + 4\nu + 1)$ είναι προφανώς σύνθετος.

36. Αν ο αριθμός $\nu > 4$ είναι σύνθετος και έχει τουλάχιστον δύο διαφορετικούς πρώτους παράγοντες, τότε γράφεται στη μορφή

$$\nu = \kappa \cdot \lambda,$$

με $\kappa < \lambda < \nu - 1$. Δηλαδή οι φυσικοί κ και λ είναι παράγοντες του γινομένου (ν-1)! και $\nu \mid (\nu - 1)!$.
Αν ο σύνθετος ν δεν έχει διαφορετικούς παράγοντες, τότε γράφεται $\nu = \kappa^\mu$ και προφανώς ο αριθμός

$$(\nu - 1)! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot \kappa(\kappa + 1) \ldots \kappa^{\mu-1} \ldots (\kappa^\mu - 1)$$

είναι πολλαπλάσιο του $\kappa \cdot \kappa^{\mu-1} = \kappa^\mu = \nu$.

37. Χωρίς βλάβη της γενικότητας, υποθέτουμε ότι ο συντελεστής του μεγιστοβάθμιου όρου του $P(x)$ είναι θετικός. Τότε, καθώς ο αριθμός x τείνει στο $+\infty$ και η αριθμητική τιμή $P(x)$ θα τείνει στο $+\infty$. Επομένως, υπάρχει φυσικός αριθμός ν με $P(\nu) > 0$. Εύκολα μπορεί κανείς να επαληθεύσει ότι για κάθε φυσικό μ, ο αριθμός $P(\nu)$ διαιρεί τον $P(\nu + \mu P(\nu))$.
Άρα υπάρχουν άπειροι φυσικοί x για τους οποίους η αριθμητική τιμή $P(x)$ είναι σύνθετος αριθμός.

38. Όμοια με την Εφαρμογή 14 § 1.6 .

39. Έστω ένας φυσικός $\alpha=4\kappa+3$. Αν είναι πρώτος , τότε η απόδειξη είναι προφανής. Αν ο α είναι σύνθετος, τότε γράφεται στη μορφή

$$\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\nu^{\alpha_\nu},$$

όπου οι $p_1 < p_2 < \dots < p_\nu$ είναι περιττοί πρώτοι αριθμοί, δηλαδή της μορφής $4\lambda+1$ ή $4\lambda+3$.
Αν όλοι είναι της μορφής $4\lambda+1$ τότε προφανώς και το γινόμενό τους θα είναι της ίδιας μορφής, άτοπο. Άρα , τουλάχιστον ένας από τους πρώτους παράγοντες του α είναι της μορφής $4\lambda+3$.
Αν θεωρήσουμε έναν φυσικό $\alpha=6\kappa+5$, καταλήγουμε στο ίδιο συμπέρασμα, εργαζόμενοι όπως παραπάνω.

40. Ας θεωρήσουμε την κανονική μορφή των α, β, γ:

$$\begin{aligned} \alpha &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa} \\ \beta &= p_1^{\beta_1} p_2^{\beta_2} \dots p_\kappa^{\beta_\kappa} \\ \gamma &= p_1^{\gamma_1} p_2^{\gamma_2} \dots p_\kappa^{\gamma_\kappa}, \end{aligned}$$

όπου κάποιοι από τους εκθέτες μπορεί να είναι μηδενικοί.
Τότε

$$\begin{aligned} \delta &= p_1^{\min\{\alpha_1,\beta_1\}} p_2^{\min\{\alpha_2,\beta_2\}} \dots p_\kappa^{\min\{\alpha_\kappa,\beta_\kappa\}} \\ \beta\cdot\gamma &= p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \dots p_\kappa^{\beta_\kappa+\gamma_\kappa} \\ \delta\cdot\gamma &= p_1^{\gamma_1+\min\{\alpha_1,\beta_1\}} p_2^{\gamma_2+\min\{\alpha_2,\beta_2\}} \dots p_\kappa^{\gamma_\kappa+\min\{\alpha_\kappa,\beta_\kappa\}}. \end{aligned}$$

Από τη σχέση $\alpha \mid \beta\gamma$, είναι φανερό ότι

$$\begin{aligned} \alpha_j &\le \beta_j + \gamma_j \qquad (j=1,2,\dots,\kappa) \text{ ή} \\ \alpha_j &\le \min\{\alpha_j,\beta_j\} + \gamma_j \quad (j=1,2,\dots,\kappa). \end{aligned}$$

Άρα $\alpha \mid \delta\gamma$.

41. Έχουμε $p^2 - q^2 = (p+q)(p-q)$.
Οι p, q θα είναι της μορφής $3\kappa+1$ ή $3\kappa+2$, αφού είναι πρώτοι αριθμοί. Αν είναι και οι δύο της ίδιας μορφής, τότε $3 \mid p-q$, ενώ αν είναι διαφορετικής μορφής , $3 \mid p+q$, άρα πάντα $3 \mid (p+q)(p-q)$.

Επίσης, επειδή οι p, q είναι περιττοί, οι αριθμοί $p+q$ και $p-q$ είναι άρτιοι. Αρκεί να αποδείξουμε ότι ένας από τους $p+q$, $p-q$ διαιρείται με τον 4. Τότε ο $(p+q)(p-q)$ θα διαιρείται με το 8, άρα και με το 24, αφού (8,3)=24.
Πράγματι, οι p, q θα είναι της μορφής $4κ+1$ ή $4κ+3$, οπότε, όπως και προηγουμένως, κάποιος τουλάχιστον από τους $p+q$, $p-q$ θα διαιρείται με τον 4.

42. Απλή, χρησιμοποιώντας το κριτήριο ρίζας.

Λύσεις Ασκήσεων § 1.7

Α' Ομάδα

1. Απλή εφαρμογή του ορισμού των τέλειων αριθμών.

2. Απλή εφαρμογή του ορισμού του δ(ν).

3. Απλή εφαρμογή του ορισμού του σ(ν).

4. Κάθε πρώτος αριθμός p έχει ακριβώς δύο διαιρέτες (τον 1 και τον p) και κάθε σύνθετος αριθμός α έχει τουλάχιστον και έναν τρίτο διαιρέτη. Άρα οι πρώτοι αριθμοί είναι οι μοναδικοί φυσικοί με ακριβώς δύο διαιρέτες.

5. Έστω ν ένας φυσικός αριθμός με κανονική μορφή

$$\nu = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_\kappa^{\alpha_\kappa}$$

και πλήθος διαιρετών

$$\delta(\nu) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_\kappa + 1) = 3.$$

Άρα $\alpha_t = 2$ για κάποιο $t \in \{1, 2, \ldots, \kappa\}$ και $\alpha_i = 0$ για κάθε $i \neq t$. Δηλαδή, ο ν είναι της μορφής $\nu = p^2$, όπου p : πρώτος.

6. Αρκεί να ελέγξουμε όλους τους φυσικούς ν=4,5,6,7,8,9, αφού $\sigma(10) > 10$. Έχουμε

$$\begin{aligned} \sigma(4) &= 1 + 2 + 4 = 7, & \sigma(5) &= 1 + 5 = 6 \\ \sigma(6) &= 1 + 2 + 3 + 6 = 12, & \sigma(7) &= 1 + 7 = 8 \\ \sigma(8) &= 1 + 2 + 4 + 8 = 15, & \sigma(9) &= 1 + 3 + 9 = 13. \end{aligned}$$

Άρα δεν υπάρχει φυσικός ν με σ(ν)=10.

7. Έστω η κανονική μορφή του ν,

$$\nu = p_1^{\nu_1} p_2^{\nu_2} \ldots p_\kappa^{\nu_\kappa} \ (p_1 < p_2 < \ldots < p_\kappa)$$

και το πλήθος των διαιρετών του

$$\delta(\nu) = (\nu_1 + 1)(\nu_2 + 1) \ldots (\nu_\kappa + 1).$$

Ο αριθμός $\delta(\nu)$ είναι πρώτος αν και μόνο αν $\kappa = 1$ και $\nu = p_1^{\nu_1}$.

Β' Ομάδα

8. Θεωρούμε τον φυσικό ν στην κανονική του μορφή

$$\nu = p_1^{\nu_1} p_2^{\nu_2} \dots p_\kappa^{\nu_\kappa} \ (p_1 < p_2 < \dots < p_\kappa).$$

Από την υπόθεση $\delta(\nu) = 12$, προκύπτει ότι
$(\nu_1 + 1)(\nu_2 + 1)\dots(\nu_\kappa + 1) = 12$.
Επιπλέον, $\kappa \leq 3$, διότι $2^4 = 16 > 12$. Επομένως ο ν γράφεται στη μορφή

$$\nu = p_1^{\nu_1} p_2^{\nu_2} p_3^{\nu_3}$$

με $0 \leq \nu_1 \leq 6$, $0 \leq \nu_2 \leq 4$ και $0 \leq \nu_3 \leq 2$ αφού $2^7 = 128 > 70$, $3^4 = 81 > 70$ και $5^3 = 125 > 70$. Λαμβάνοντας υπόψη μας και τη σχέση $(\nu_1 + 1)(\nu_2 + 1)\dots(\nu_\kappa + 1) = 12$ καταλήγουμε στο ότι ο μοναδικός φυσικός που είναι μικρότερος ή ίσος του 70 και έχει 12 ακριβώς διαιρέτες είναι ο $2^2 \cdot 3 \cdot 5 = 60$.

9. Αν $\kappa_1 = 1, \kappa_2, \dots, \kappa_\nu = \alpha$ είναι όλοι οι παράγοντες του φυσικού α, τότε

$$\begin{aligned} \alpha \cdot \left(\tfrac{1}{\kappa_1} + \tfrac{1}{\kappa_2} + \dots + \tfrac{1}{\kappa_\nu}\right) &= \tfrac{\alpha}{\kappa_1} + \tfrac{\alpha}{\kappa_2} + \dots + \tfrac{\alpha}{\kappa_\nu} \\ &= \kappa_\nu + \kappa_{\nu-1} + \dots + \kappa_1 \\ &= \sigma(\alpha). \end{aligned}$$

10. Έστω $\nu = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_\kappa^{\alpha_\kappa}$ η κανονική γραφή του φυσικού $\nu > 1$.
Έχουμε

$$\begin{aligned} \left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\dots\left(1 - \tfrac{1}{p_\kappa}\right) &= \frac{(p_1-1)(p_2-1)\cdot\dots\cdot(p_\kappa-1)}{p_1 \cdot p_2 \cdot \dots \cdot p_\kappa} \\ &= \frac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_\kappa^{\alpha_\kappa}}{\left(\frac{p_1^{\alpha_1+1} \cdot p_2^{\alpha_2+1} \cdot \dots \cdot p_\kappa^{\alpha_\kappa+1}}{(p_1-1)(p_2-1)\dots(p_\kappa-1)}\right)} \\ &= \frac{\nu}{\left(\frac{p_1^{\alpha_1+1}}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}}{p_2-1}\right)\dots\left(\frac{p_\kappa^{\alpha_\kappa+1}}{p_\kappa-1}\right)} \\ &< \frac{\nu}{\left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\dots\left(\frac{p_\kappa^{\alpha_\kappa+1}-1}{p_\kappa-1}\right)}. \end{aligned}$$

Άρα $\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{p_\kappa}\right) < \frac{\nu}{\sigma(\nu)} < 1$.

11. Για έναν σύνθετο $\nu > 1$, έχουμε

$$\begin{aligned}\sigma(\nu) &= \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right)\left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right)\ldots\left(\frac{p_\varkappa^{\alpha_\varkappa+1}-1}{p_\varkappa-1}\right)\\ &= \left(p_1^{\alpha_1}+p_1^{\alpha_1-1}+\ldots+1\right)\left(p_2^{\alpha_2}+p_2^{\alpha_2-1}+\ldots+1\right)\ldots\\ &\quad\ldots\left(p_\varkappa^{\alpha_\varkappa}+p_\varkappa^{\alpha_\varkappa-1}+\ldots+1\right).\end{aligned}$$

Κάνοντας τις πράξεις καταλήγουμε ότι

$$\begin{aligned}\sigma(\nu) &= (p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_\varkappa^{\alpha_\varkappa})+\left(p_1^{\alpha_1-1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_\varkappa^{\alpha_\varkappa}\right)+\\ &\quad+\left(p_1^{\alpha_1}\cdot p_2^{\alpha_2-1}\cdot\ldots\cdot p_\varkappa^{\alpha_\varkappa}\right)+\ldots+p_1+p_2+\ldots+p_\varkappa+1,\end{aligned}$$

δηλαδή

$$\sigma(\nu)=\nu+\left(\frac{\nu}{p_1}+\frac{\nu}{p_2}+\ldots+\frac{\nu}{p_\varkappa}\right)+\ldots+p_\varkappa+1>\nu+\sqrt{\nu}.$$

12. Αρκεί να παρατηρήσουμε ότι για κάθε περιττό πρώτο p, ο αριθμός 2^{p-1} είναι της μορφής $3\nu+1$.

13. Αρκεί να μελετήσουμε τα υπόλοιπα των δυνάμεων του 2 με το 100.

14. Έστω $\nu = p_1^{\alpha_1}\cdot p_2^{\alpha_2}\ldots p_r^{\alpha_r}$. Τότε έχουμε ότι:

$$\delta(\nu)=(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)$$

$$\delta(\nu^2)=(2\alpha_1+1)(2\alpha_2+1)\ldots(2\alpha_r+1).$$

Επομένως τα α_i πρέπει να επιλεγούν έτσι ώστε:

$$(2\alpha_1+1)(2\alpha_2+1)\ldots(2\alpha_\nu+1)=\varkappa(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_\nu+1).$$

Αφού οι $(2\alpha_i+1)$ είναι περιττοί, θα πρέπει και ο $\varkappa$ να είναι περιττός. Αντίστροφα, θα αποδείξουμε ότι για οποινδήποτε δοσμένο περιττό $\varkappa$, μπορούμε να επιλέξουμε κατάλληλα α_i, ώστε να ισχύει η ζητούμενη σχέση.
Χρησιμοποιούμε μία μορφή επαγωγής για $\nu=\varkappa$. Αρχικά, ισχύει για $\varkappa=1$ (θεωρούμε $\nu=1$). Κατόπιν, θα αποδείξουμε ότι αν ισχύει για $\varkappa$, τότε θα ισχύει για το $(2^m\varkappa-1)$, το οποίο αρκεί, αφού κάθε

περιττός γράφεται στη μορφή $(2^m x - 1)$ για κάποιον μικρότερο περιττό x.
Θεωρούμε

$$\alpha_i = 2^i((2^m - 1) - 1), \quad \gamma\iota\alpha i = 0, 1, \ldots, m - 1.$$

Τότε

$$\begin{aligned} 2\alpha_i + 1 &= 2^{i+1}(2^m - 1)x - (2^{i+1} - 1) \\ \alpha_i + 1 &= 2^i(2^m - 1)x - (2^i - 1) \end{aligned}$$

Άρα το γινόμενο των $(2\alpha_i+1)$ διαιρείται με το γινόμενο των (α_i+1) δίνει:

$$\frac{2^m(2^m - 1)x - (2^m - 1)}{(2^m - 1)x} = \frac{2^m x - 1}{x}.$$

Αν επιλέξουμε λοιπόν τα α_i που δίνουν τον x, έχουμε τον $2^m x - 1$ και η επαγωγή έχει ολοκληρωθεί.

Λύσεις Γενικών Ασκήσεων του 1ου Κεφαλαίου

1. Αν ένας φυσικός ν είναι περιττός, τότε

$$\nu = 2\kappa + 1 = \kappa + (\kappa + 1).$$

Δηλαδή, γράφεται ως άθροισμα δύο διαδοχικών φυσικών αριθμών. Αν ένας φυσικός ν είναι γινόμενο ενός άρτιου λ και ενός περιττού μ, τότε επαληθεύεται εύκολα ότι

$$\nu = \mu\lambda = \left(\lambda - \frac{\mu-1}{2}\right) + \left(\lambda - \frac{\mu-3}{2}\right) + \ldots + \lambda + \ldots + \left(\lambda + \frac{\mu-1}{2}\right).$$

Δηλαδή, γράφεται ως άθροισμα μ διαδοχικών φυσικών αριθμών. Τέλος, μπορεί κανείς να παρατηρήσει από την Εφ. 9 §1.1, ότι καμμιά δύναμη του 2 δεν γράφεται ως άθροισμα διαδοχικών φυσικών.

2. Ο αριθμός N γράφεται

$$\begin{aligned} N &= 11^{10} - 1 \\ &= (11-1)(11^9 + 11^8 + \ldots + 11 + 1) \\ &= 10(11^9 + 11^8 + \ldots + 11 + 1). \end{aligned}$$

Το άθροισμα $11^9 + 11^8 + \ldots + 11 + 1$ αποτελείται από 10 όρους και το τελευταίο ψηφίο κάθε όρου είναι το 1. Επομένως, έχουμε ότι

$$\begin{aligned} 11^9 + 11^8 + \ldots + 11 + 1 &= 10\kappa + \underbrace{1 + 1 + \ldots + 1}_{10-\mu ονάδες} \\ &= 10\kappa + 10 \end{aligned}$$

και $N = 10 \cdot 10(\kappa + 1) = 100(\kappa + 1)$.

3. Αφού ο ν δεν είναι πολλαπλάσιο του 2 ή του 3, θα είναι της μορφής $6\kappa + 1$ ή $6\kappa + 5$.

Αν $\nu = 6\kappa + 1$, τότε

$$\frac{\nu^2 + 23}{24} = \frac{36\kappa^2 + 12\kappa + 24}{24} = \frac{(3\kappa + 1)\kappa}{2} + 1.$$

Αν $\nu = 6x + 5$, τότε

$$\frac{\nu^2 + 23}{24} = \frac{36x^2 + 60x + 48}{24} = \frac{(3x + 5)x}{2} + 2.$$

Οι αριθμοί $(3x + 1)x$ και $(3x + 5)x$ είναι άρτιοι για κάθε ακέραιο x και η απόδειξη ολοκληρώθηκε.

4. Αποδεικνύουμε ότι ο αριθμός 54 διαιρεί τον

$$\begin{aligned} N &= (\nu^3 - 1)\nu^3(\nu^3 + 1) \\ &= (\nu - 1)\nu^3(\nu + 1)(\nu^2 + \nu + 1)(\nu^2 - \nu + 1). \end{aligned}$$

5. Είναι διαδοχικά :

$$\underbrace{11\ldots111}_{1997}\ \underbrace{22\ldots2}_{1998}5 = \underbrace{11\ldots111}_{1997}\cdot 10^{1999} + \underbrace{22\ldots2}_{1998}\cdot 10 + 5$$

$$= \tfrac{10^{1997}-1}{9}10^{1999} + 2\tfrac{10^{1998}-1}{9}10 + 5$$

$$= \tfrac{1}{9}\left(10^{3996} - 10^{1999} + 2\cdot 10^{1999} - 20 + 45\right)$$

$$= \tfrac{1}{9}\left(10^{3996} + 2\cdot 5\cdot 10^{1998} + 25\right)$$

$$= \tfrac{1}{9}\left(10^{1998} + 5\right)^2$$

$$= \left(\tfrac{10^{1998}+5}{3}\right)^2$$

δηλαδή, είναι τέλειο τετράγωνο ακεραίου αφού το άθροισμα των ψηφίων του αριθμού $(10^{1998} + 5)$ διαιρείται με τον 3.

6. Παρατηρούμε ότι $1441 = 11 \cdot 131$ και για αυτό πρέπει
   $11 \mid (60^\nu + x \cdot 71^\nu)$ και $131 \mid (60^\nu + x \cdot 70^\nu)$.
   Επειδή $60^\nu + x \cdot 71^\nu = (60^\nu - 71^\nu) + (x+1)71^\nu$ και ο αριθμός ο $60^\nu - 71^\nu = (60 - 71)(60^{\nu-1} + 60^{\nu-2} \cdot 71 + \ldots + 71^{\nu-1})$ είναι πολλαπλάσιο του 11, πρέπει και ο $(x+1)71^\nu$ να είναι πολλαπλάσιο του 11.
   Όμως $(71, 11) = 1$, άρα πρέπει $11 \mid (x + 1)$.
   Ανάλογα, έχουμε ότι: $60^\nu + x \cdot 71^\nu = (60^\nu + 71^\nu) + (x-1)71^\nu$ και

επειδή για περιττό ν , είναι $60^\nu+71^\nu = (60+71)(60^{\nu-1}-\ldots+71^{\nu-1})$, καταλήγουμε ότι $131 \mid (\varkappa - 1)$.
Επομένως, υπάρχουν κατάλληλοι φυσικοί α και β τέτοιοι ώστε $\varkappa = 11\alpha - 1$ και $\varkappa = 131\beta + 1$.
Άρα

$$11\alpha - 1 = 131\beta + 1 \text{ ή}$$

$$\alpha = \frac{131\beta + 2}{11} = \frac{132\beta - \beta + 2}{11} = 12 + \frac{2-\beta}{11}.$$

Για $\beta = 2$ παίρνουμε $\alpha = 24$ και $\varkappa = 263$ που είναι η ζητούμενη μικρότερη τιμή του $\varkappa$.

7. Παρατηρούμε ότι $-\frac{2}{3} = \frac{1}{3} - \frac{3}{3}, -\frac{2}{6} = \frac{1}{6} - (\frac{3}{3})(\frac{1}{2}), -\frac{2}{9} = \frac{1}{9} - (\frac{3}{3})(\frac{1}{3}), \ldots,$ κ.ο.κ. Άρα έχουμε

$$\begin{aligned}
\tfrac{\mu}{\nu} &= 1 + \tfrac{1}{2} - \tfrac{2}{3} + \tfrac{1}{4} + \tfrac{1}{5} - \tfrac{2}{6} + \ldots + \tfrac{1}{478} + \tfrac{1}{479} - \tfrac{2}{480} \\
&= 1 + \tfrac{1}{2} + \tfrac{1}{3} + \tfrac{1}{4} + \tfrac{1}{5} + \ldots + \tfrac{1}{480} - (\tfrac{3}{3})(1 + \tfrac{1}{2} + \tfrac{1}{3} + \ldots + \tfrac{1}{160}) \\
&= \tfrac{1}{161} + \tfrac{1}{162} + \tfrac{1}{163} + \ldots + \tfrac{1}{479} + \tfrac{1}{480} \\
&= (\tfrac{1}{161} + \tfrac{1}{480}) + (\tfrac{1}{162} + \tfrac{1}{479}) + \ldots + (\tfrac{1}{320} + \tfrac{1}{321}) \\
&= \tfrac{641}{161\cdot 480} + \tfrac{641}{162\cdot 479} + \ldots + \tfrac{641}{320\cdot 321} \\
&= 641(\tfrac{1}{161\cdot 480} + \tfrac{1}{162\cdot 479} + \ldots + \tfrac{1}{320\cdot 321}).
\end{aligned}$$

Δηλαδή το πηλίκο μ/ν γράφεται

$$\frac{\mu}{\nu} = \frac{641 \cdot M}{161 \cdot 162 \cdot 163 \cdot \ldots \cdot 479 \cdot 480}$$

Άρα $641 \mid \mu$, αφού ο 641 είναι σχετικά πρώτος με τους αριθμούς 161,162,...

8. Έστω α το πλήθος των ζώων. Από τα λεγόμενα του κτηνοτρόφου προκύπτει ότι υπάρχουν φυσικοί x και y τέτοιοι ώστε

$$\alpha = 12x + 9 \text{ και } \alpha = 16y + 5.$$

Επομένως, έχουμε τη γραμμική Διοφαντική εξίσωση

$$12x + 9 = 16y + 5 \text{ ή}$$

$$-12x + 16y = 4.$$

Αφού $(-12, 16) = 4$ και $4 \mid 4$, η εξίσωση έχει λύση και παρατηρούμε ότι

$$-12 \cdot 1 + 16 \cdot 1 = 4.$$

Δηλαδή μια λύση της Διοφαντικής εξίσωσης είναι $x_0 = 1$, $y_0 = 1$.
Άρα η εξίσωση έχει άπειρες λύσεις της μορφής:

$$\begin{aligned} x &= 1 + 4t \\ y &= 1 + 3t, \end{aligned}$$

όπου $t \in Z$.
Επιπλέον έχουμε τους περιορισμούς

$$250 < 12x + 9 < 300 \quad \text{και} \quad 250 < 16y + 5 < 300 \quad \text{ή}$$
$$250 < 12 + 48t + 9 < 300 \quad \text{και} \quad 250 < 16 + 48t + 5 < 300 \quad \text{ή}$$

$$\tfrac{229}{48} < t < \tfrac{279}{48}.$$

Άρα $t = 5$, $x = 21$, $y = 16$ και $\alpha = 261$.

9. Αν ο α είναι περιττός, δηλαδή της μορφής $\alpha = 2x + 1$, τότε ο αριθμός

$$\alpha^\nu + 1 = (2x + 1)^\nu + 1 = 2(2^{\nu-1}x^\nu + \nu 2^{\nu-2}x^{\nu-1} + \ldots + \nu x + 1)$$

είναι σύνθετος.

Αν ο ν έχει έναν περιττό διαιρέτη δ και γράφεται $\nu = \mu\delta$, τότε ο αριθμός

$$\alpha^\nu + 1 = (\alpha^\mu)^\delta + 1 = (\alpha^\mu + 1)[(\alpha^\mu)^{\delta-1} + \ldots + \alpha^\mu + 1]$$

είναι σύνθετος.

Επομένως, αν ο $\alpha^\nu + 1$ είναι πρώτος, τότε ο α πρέπει να είναι άρτιος και ο ν πρέπει να είναι δύναμη του 2.

10. Από το ανάπτυγμα του Νεύτωνα γνωρίζουμε ότι
$(\mu+\nu)^p = \mu^p + \nu^p + p(\ldots)$. Επομένως, ισχύει ότι αν $p \mid (\mu^p+\nu^p)$, τότε $p \mid (\mu+\nu)^p$, δηλάδη $p \mid (\mu+\nu)$.
Δηλαδή, υπάρχει φυσικός κ τέτοιος ώστε $\mu+\nu = \kappa p$ και

$$\begin{aligned}\mu^p + \nu^p &= \mu^p + (\kappa p - \mu)^p \\ &= \mu^p + (\kappa p)^p - p(\kappa p)^{p-1}\mu + \ldots + p(\kappa p)\mu^{p-1} - \mu^p \\ &= p^2(\kappa^p p^{p-2} - \kappa^{p-1}p^{p-2}\mu + \ldots + \kappa\mu^{p-1})\end{aligned}$$

Άρα $p^2 \mid (\mu^p+\nu^p)$.

11. Έστω $\delta = (\alpha^2+\beta^2, \alpha+\beta)$ και $(\alpha,\beta)=1$. Τότε $\delta \mid (\alpha^2+\beta^2)$ και $\delta \mid (\alpha+\beta)$, δηλαδή $\delta \mid (\alpha^2+\beta^2)$ και $\delta \mid (\alpha+\beta)^2$.
Άρα $\delta \mid [(\alpha+\beta)^2 - (\alpha^2+\beta^2]$, οπότε $\delta \mid (2\alpha\beta)$.
Αν $p \geq 3$ είναι ένας πρώτος παράγοντας του δ, τότε $p \mid \alpha$ ή $p \mid \beta$ και δεδομένου ότι $p \mid (\alpha+\beta)$, προκύπτει ότι ο p είναι κοινός διαιρέτης των α και β, άτοπο διότι $(\alpha,\beta)=1$.
Επομένως, ο δ είναι της μορφής $\delta = 2^\kappa$. Επιπλέον οι αριθμοί α και β δεν είναι άρτιοι και οι δύο, αφού $(\alpha,\beta)=1$.
Αν οι α και β είναι διαφορετικής αρτιότητας, τότε το άθροισμα $\alpha+\beta$ είναι περιττός και $\delta = 1$.
Αν οι α και β είναι περιττοί, τότε το άθροισμα $\alpha+\beta$ είναι άρτιος αλλά όχι πολλαπλάσιο του 4, άρα $\delta = 2$.

12. Προφανώς

$$\alpha^3+\beta^3 = (\alpha+\beta)(\alpha^2-\alpha\beta+\beta^2) = (\alpha+\beta)(\alpha^2+\beta^2) - \alpha\beta(\alpha+\beta)$$

και από την Πρόταση 1.3.1 έχουμε ότι

$$\begin{aligned}(\alpha^3+\beta^3,\ \alpha^2+\beta^2) &= (\alpha\beta(\alpha+\beta),\ \alpha^2+\beta^2) \\ &= (\alpha^2\beta+\alpha\beta^2,\ \alpha^2+\beta^2) \\ &= (\alpha^2\beta+\alpha\beta^2 - \alpha(\alpha^2+\beta^2),\ \alpha^2+\beta^2) \\ &= (\alpha^2(\beta-\alpha),\ \alpha^2+\beta^2).\end{aligned}$$

Ο $\delta = (\alpha^2(\beta-\alpha),\ \alpha^2+\beta^2)$ διαιρεί τον αριθμό $\alpha^2(\beta-\alpha)$ και αρκεί να αποδειχθεί ότι $(\delta,\alpha^2)=1$.
Πράγματι αν p είναι ένας πρώτος κοινός διαιρέτης των δ και α^2, τότε $p \mid \alpha^2$, $p \mid (\alpha^2+\beta^2)$, άρα $p \mid \beta^2$. Επομένως $p \mid (\alpha^2,\beta^2)$, οπότε προκύπτει ότι $p \mid (\alpha,\beta)$, άτοπο.

13. Θεωρούμε την κατάλληλη γραφή σε γινόμενα πρώτων παραγόντων

$$\begin{aligned}
\alpha &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa} \\
\beta &= p_1^{\beta_1} p_2^{\beta_2} \dots p_\kappa^{\beta_\kappa} \\
\alpha^\nu &= p_1^{\nu\alpha_1} p_2^{\nu\alpha_2} \dots p_\kappa^{\nu\alpha_\kappa} \\
\beta^\nu &= p_1^{\nu\beta_1} p_2^{\nu\beta_2} \dots p_\kappa^{\nu\beta_\kappa} \\
(\alpha,\beta) &= p_1^{min\{\alpha_1,\beta_1\}} p_2^{min\{\alpha_2,\beta_2\}} \dots p_\kappa^{min\{\alpha_\kappa,\beta_\nu\}} \\
(\alpha^\nu,\beta^\nu) &= p_1^{min\{\nu\alpha_1,\nu\beta_1\}} p_2^{min\{\nu\alpha_2,\nu\beta_2\}} \dots p_\kappa^{min\{\nu\alpha_\kappa,\nu\beta_\nu\}}
\end{aligned}$$

με μη αρνητικούς εκθέτες και η απόδειξη είναι άμεση.

14. Γράφουμε τους α, β και γ ως γινόμενα πρώτων παραγόντων

$$\begin{aligned}
\alpha &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa} \\
\beta &= p_1^{\beta_1} p_2^{\beta_2} \dots p_\kappa^{\beta_\kappa} \\
\gamma &= p_1^{\gamma_1} p_2^{\gamma_2} \dots p_\kappa^{\gamma_\kappa}
\end{aligned}$$

με μη αρνητικούς εκθέτες. Τότε έχουμε

$$\begin{aligned}
\beta\gamma &= p_1^{\beta_1+\gamma_1} p_2^{\beta_2+\gamma_2} \dots p_\kappa^{\beta_\kappa+\gamma_\kappa} \\
(\alpha,\beta) &= p_1^{min(\alpha_1,\beta_1)} p_2^{min\{\alpha_2,\beta_2\}} \dots p_\kappa^{min(\alpha_\kappa,\beta_\nu)} \\
(\alpha,\beta\gamma) &= p_1^{min\{\alpha_1,\beta_1+\gamma_1\}} p_2^{min\{\alpha_2,\beta_2+\gamma_2\}} \dots p_\kappa^{min\{\alpha_\kappa,\beta_\nu+\gamma_\nu\}}
\end{aligned}$$

και η απόδειξη είναι άμεση.

15. Αν το ελάχιστο κοινό πολλαπλάσιο $[\alpha,\beta]$ διαιρεί τέλεια τον γ, τότε είναι προφανές ότι $\alpha \mid \gamma$ και $\beta \mid \gamma$.
Αντίστροφα, ας υποθέσουμε ότι $\alpha \mid \beta$ και $\beta \mid \gamma$ και ας γράψουμε τους α, β, γ ως γινόμενο πρώτων παραγόντων

$$\begin{aligned}
\alpha &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa} \\
\beta &= p_1^{\beta_1} p_2^{\beta_2} \dots p_\kappa^{\beta_\kappa} \\
\gamma &= p_1^{\gamma_1} p_2^{\gamma_2} \dots p_\kappa^{\gamma_\kappa},
\end{aligned}$$

όπου οι εκθέτες είναι μη αρνητικοί. Αφού $\alpha \mid \beta$ και $\beta \mid \gamma$, έχουμε ότι $\alpha_1 \le \gamma_1$, $\alpha_2 \le \gamma_2$, ..., $\alpha_\kappa \le \gamma_\kappa$ και $\beta_1 \le \gamma_1$, $\beta_2 \le \gamma_2$, ..., $\beta_\kappa \le \gamma_\kappa$.
Έτσι για κάθε $j = 1, 2, \dots, \kappa$ προκύπτει ότι $max\{\alpha_j, \beta_j\} \le \gamma_j$, άρα $[\alpha,\beta] \mid \gamma$.

16. Γράφουμε τους α και β στην κανονική τους μορφή.

$$\begin{aligned} \alpha &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\varkappa^{\alpha_\varkappa} \quad (p_1 < p_2 < \dots < p_\varkappa) \\ \beta &= q_1^{\beta_1} q_2^{\beta_2} \dots q_\mu^{\beta_\mu} \quad (q_1 < q_2 < \dots < q_\mu) \end{aligned}$$

με θετικούς εκθέτες και $p_i \neq q_j$ για κάθε $i = 1, 2, \dots, \varkappa$ και $j = 1, 2, \dots, \mu$.
Ο φυσικός $\alpha \cdot \beta = p_1^{\alpha_1} \dots p_\varkappa^{\alpha_\varkappa} q_1^{\beta_1} \dots q_\mu^{\beta_\mu} = \gamma^\nu$ είναι τέλεια (ν-οστής τάξης) δύναμη του φυσικού γ.
Για το λόγο αυτό πρέπει όλοι οι εκθέτες να είναι πολλαπλάσια του ν, δηλαδή

$$\alpha_i = \nu\alpha_i', \;\; i = 1, 2, \dots, \varkappa$$

και

$$\beta_j = \nu\beta_j', \;\; j = 1, 2, \dots, \mu.$$

Επομένως, $\alpha = (p_1^{\alpha_1'} p_2^{\alpha_2'} \dots p_\varkappa^{\alpha_\varkappa'})^\nu$ και $\beta = (q_1^{\beta_1'} q_2^{\beta_2'} \dots q_\mu^{\beta_\mu'})^\nu$, οπότε επιλέγουμε $\delta = p_1^{\alpha_1'} p_2^{\alpha_2'} \dots p_\varkappa^{\alpha_\varkappa'}$ και $\varepsilon = q_1^{\beta_1'} q_2^{\beta_2'} \dots q_\mu^{\beta_\mu'}$.

17. Έχουμε $3^{6\nu} - 2^{6\nu} = 27^{2\nu} - 8^{2\nu}$, και επειδή ο εκθέτης 2ν είναι άρτιος, ο αριθμός αυτός θα διαιρείται με τους $27 - 8 = 19$ και $27 + 8 = 35$, αφού αυτοί οι όροι εμφανίζονται στην παραγοντοποίηση της παράστασης.
Επειδή οι αριθμοί αυτοί είναι πρώτοι μεταξύ τους, ο αριθμός θα διαιρείται και με το $19 \cdot 35 = 665$.

18. Έχουμε ότι:

$$\begin{aligned} &1 + \tfrac{1}{2^3} + \tfrac{1}{3^3} + \dots + \tfrac{1}{(p-1)^3} = \\ &= \left(1 + \tfrac{1}{(p-1)^3}\right) + \left(\tfrac{1}{2^3} + \tfrac{1}{(p-2)^3}\right) + \dots + \left(\tfrac{1}{\left(\frac{p-1}{2}\right)^3} + \tfrac{1}{\left(\frac{p+1}{2}\right)^3}\right) \end{aligned}$$

Κάθε όρος στις παρενθέσεις είναι της μορφής:

$$\left(\frac{1}{\varkappa^3} + \frac{1}{(p-\varkappa)^3}\right) = \frac{p(p^2 - 3p\varkappa + 3\varkappa^2)}{\varkappa^3(p-\varkappa)^3}$$

Επειδή ο p δεν εμφανίζεται σε κανένα παρανομαστή αλλά εμφανίζεται σε όλους τους αριθμητές αυτών των κλασμάτων, συμπεραίνουμε ότι ο p διαιρεί τον αριθμητή μ.

19. Αν έχουμε 4 διαδοχικούς "ενδιαφέροντες" αριθμούς, τότε ένας από αυτούς θα είναι της μορφής $4x$, ο οποίος είναι "ενδιαφέρον" αν και μόνο αν $x = 1$. Αλλά ούτε ο 3 ούτε ο 5 δεν είναι "ενδιαφέροντες", αδύνατο.
'Ετσι θα έχουμε το πολύ 3 διαδοχικούς "ενδιαφέροντες" αριθμούς. Οι τρεις αριθμοί $33 = 3 \cdot 11$, $34 = 2 \cdot 17$, $35 = 5 \cdot 7$ είναι όλοι "ενδιαφέροντες", οπότε η απάντηση είναι 3.

20. 'Εστω ότι υπάρχουν φυσικοί αριθμοί ν, x τέτοιοι ώστε

$$2^{2^\nu} + 1 = x^3.$$

Τότε προφανώς ο x είναι περιττός και

$$2^{2^\nu} = x^3 - 1 = (x-1)(x^2 + x + 1),$$

οπότε $x - 1 = 2^\lambda$ και $x^2 + x + 1 = 2^\mu$, λ, μ φυσικοί με $\lambda + \mu = 2^\nu$.
'Εχουμε διαδοχικά $2^\mu - 2^{2\lambda} = x^2 + x + 1 - (x-1)^2 = 3x$.
Ο αριθμός $3x$ είναι περιττός ενώ ο $2^\mu - 2^{2\lambda}$ για $\mu \geq 1$, $\lambda \geq 1$ είναι άρτιος, άτοπο.
Για $\mu = 0$ έχουμε ότι $x^2 + x + 1 = 1$, άρα $x = 0$, άτοπο, αφού $x =$περιττός.
Για $\lambda = 0$ έχουμε ότι $x - 1 = 1$, άρα $x = 2$, άτοπο.
'Ετσι συμπεραίνουμε ότι κανένας από τους αριθμούς α_ν δεν είναι κύβος ακεραίων.

21. Η εξίσωση $x^y = y^x$ εκφράζει ότι οι x και y πρέπει να έχουν τους ίδιους πρώτους παράγοντες.
'Εστω

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_\kappa^{\alpha_\kappa}$$

και

$$y = p_1^{\beta_1} p_2^{\beta_2} \dots p_\kappa^{\beta_\kappa}$$

η ανάλυση των x, y σε πρώτους παράγοντες.
Τότε αφού $x^y = y^x$ έχουμε ότι:

$$\begin{aligned} x^y = y^x \Longrightarrow \quad & \alpha_1 y = \beta_1 x \\ & \alpha_2 y = \beta_2 x \\ & \vdots \\ & \alpha_\kappa y = \beta_\kappa x. \end{aligned}$$

Έστω (χωρίς βλάβη της γενικότητας) ότι $y > x$. Τότε ο x διαιρεί τον y, δηλαδή $y = \kappa x$ για κάποιον ακέραιο κ. Τότε πρέπει

$$x^{\kappa x} = (\kappa x)^x \quad \acute{\eta} \quad x^{\kappa-1} = \kappa.$$

Επειδή $y > x$, πρέπει $\kappa > 1$, οπότε $x > 1$. Όμως $2^{2-1} = 2$ και για $\kappa > 2$ έχουμε $x^{\kappa-1} > \kappa$, αφού

$$x^{\kappa-1} \geq 2^{\kappa-1} > \kappa.$$

Άρα οι μόνες λύσεις της εξίσωσης είναι $x = 2$, $y = 4$.

22. Επειδή

$$\alpha^\nu - \beta^\nu = (\alpha - \beta)(\alpha^{\nu-1} + \alpha^{\nu-2}\beta + \ldots + \beta^{\nu-1})$$

για όλους τους ακεραίους $\alpha \neq \beta$, ο αριθμός $P(\alpha) - P(\beta)$ διαιρείται με το $\alpha - \beta$ για κάθε πολυώνυμο $P(x)$ με ακέραιους συντελεστές. Άρα ο $P(\nu) - P(-\nu) \neq 0$ διαιρείται με το 2ν συνεπώς

$$P(\nu) - P(-\nu) \geq 2\nu \quad \acute{\eta}$$
$$P(-\nu) \leq P(\nu) - 2\nu.$$

Άρα

$$P(-\nu) < \nu - 2\nu \quad \acute{\eta}$$
$$P(-\nu) < -\nu.$$

23. Έχουμε

$$\nu^{12} - \nu^8 - \nu^4 + 1 = (\nu^4 + 1)(\nu^2 + 1)^2(\nu - 1)^2(\nu + 1)^2.$$

Ο αριθμός $(\nu^4 + 1)(\nu^2 + 1)^2$ διαιρείται με το 2^3 και ένας από τους άρτιους αριθμούς $\nu-1$, $\nu+1$ διαιρείται με το 4, άρα ο $(\nu-1)^2(\nu+1)^2$ διαιρείται με το 2^6.
Έτσι ο αριθμός $\nu^{12} - \nu^8 - \nu^4 + 1$ διαιρείται με το $2^9 = 512$.

24. Παρατηρούμε ότι αν θέσουμε $\alpha = 4\kappa^4$, $\kappa \geq 2$, τότε ο αριθμός z παραγοντοποιείται ως εξής:

$$\begin{aligned} z = \nu^4 + 4\kappa^4 &= \nu^4 + 4\nu^2\kappa^2 + 4\kappa^2 - 4\nu^2\kappa^2 \\ &= (\nu^2 + 2\kappa^2)^2 - (2\nu\kappa)^2 \\ &= (\nu^2 + 2\kappa^2 + 2\nu\kappa)(\nu^2 + 2\kappa^2 - 2\nu\kappa). \end{aligned}$$

Αρκεί να αποδείξουμε ότι οι παράγοντες είναι μεγαλύτεροι του 1. Πράγματι,

$$\nu^2 + 2x^2 + 2\nu x \geq \nu^2 + 2x^2 - 2\nu x = (\nu - x)^2 + x^2 \geq x^2 \geq 4.$$

25. Ο $\nu = 1$ είναι μία δυνατή τιμή αφού ο 2 διαιρεί το 8.
Για $\nu \geq 2$ έχουμε ότι

$$\alpha_\nu = (3+5)\alpha_{\nu-1} - 15\alpha_{\nu-2}$$

όπου $\alpha_\nu = 3^\nu + 5^\nu$.
Αν ο $\alpha_{\nu-1}$ διαιρεί τον α_ν, θα πρέπει να διαιρεί και τον $15\alpha_{\nu-2}$. Επειδή όμως ο $\alpha_{\nu-1}$ είναι σχετικά πρώτος με τους 3 και 5, θα πρέπει να διαιρεί τον $\alpha_{\nu-2}$, αδύνατο, αφού ο $\alpha_{\nu-1}$ είναι μεγαλύτερος του $\alpha_{\nu-2}$.

26. Έχουμε διαδοχικά:

$$\begin{aligned}
&2222^{5555} + 5555^{2222} = \\
&= (2222^{5555} + 4^{5555}) + (5555^{2222} - 4^{2222}) - (4^{5555} - 4^{2222}) \\
&= (2222 + 4)(2222^{5554} - \ldots + 4^{5554}) + \\
&\quad + (5555 - 4)(5555^{2221} + \ldots + 4^{2221}) - 4^{2222}(4^{3333} - 1).
\end{aligned}$$

Όμως

$$\begin{aligned}
2222 + 4 &= 7 \cdot 318 \\
5555 - 4 &= 7 \cdot 793 \\
4^{3333} - 1 &= 64^{1111} - 1 = (64-1)(64^{1110} + \ldots + 1) \\
&= 7 \cdot 9 \cdot (64^{1110} + \ldots + 1),
\end{aligned}$$

οπότε ο αριθμός $2222^{5555} + 5555^{2222}$ διαιρείται με το 7.

27. Επειδή $(\alpha, \beta) = 1$ αν και μόνο αν $(\alpha, \alpha + \beta) = 1$ αρκεί να θεωρήσουμε $1 \leq \alpha \leq 7250$.
Ας μετρήσουμε το πλήθος των αριθμών α με $1 \leq \alpha \leq 7250$ και $(\alpha, 7250) = 1$.
Οι διαιρέτες του 7250 είναι 2, 5, και 29.

Το πλήθος των αριθμών που διαιρούνται

$$\begin{aligned}
&\mu\varepsilon\ \tau o\ 2\ \varepsilon\acute{\iota}\nu\alpha\iota\ 7250\ /2 = 3625\\
&\mu\varepsilon\ \tau o\ 5 : 7250/5 = 1450\\
&\mu\varepsilon\ \tau o\ 29 : 7250/5 = 250\\
&\mu\varepsilon\ \tau o\ 2\ \kappa\alpha\iota\ \tau o\ 5 : 7250/10 = 725\\
&\mu\varepsilon\ \tau o\ 2\ \kappa\alpha\iota\ \tau o\ 29 : 7250/58 = 125\\
&\mu\varepsilon\ \tau o\ 5\ \kappa\alpha\iota\ \tau o\ 29 : 7250/145 = 50\\
&\mu\varepsilon\ \tau o\ 2, 5\ \kappa\alpha\iota\ \tau o\ 29 : 7250/290 = 25.
\end{aligned}$$

Άρα το πλήθος των αριθμών αυτών είναι

$$3625 + 1450 + 250 - 725 - 125 - 50 + 25 = 4450.$$

Άρα το ζητούμενο πλήθος είναι $7250 - 4450 = 2800$.

28. Θεωρούμε τους αριθμούς $\alpha_\nu = p^{p^\nu - 1}$, όπου p ένας τυχαίος πρώτος, για $\nu = 1, 2, 3, \ldots$
Για τους αριθμούς αυτούς ισχύει $\delta(\alpha_\nu) = p^\nu$, άρα

$$\frac{\alpha_\nu}{\delta(\alpha_\nu)} = p^{p^\nu - \nu - 1},$$

ο οποίος είναι ακέραιος, αφού για $p = 2^\nu = (1+1)^\nu \geq 1 + \nu$ (ισχύει και για $\nu = 1$), ενώ για $p \geq 3$ έχουμε ότι

$$p^\nu > e^\nu \geq \nu + 1.$$

29. Έστω ο φυσικός αριθμός

$$\alpha = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa} \quad (p_1 < p_2 < \ldots < p_\kappa)$$

στην κανονική του μορφή και

$$\sigma(\alpha) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \ldots \frac{p_\kappa^{\alpha_\kappa+1} - 1}{p_\kappa - 1}$$

το άθροισμα των διαιρετών του. Ο αριθμός $\sigma(\alpha)$ είναι περιττός αν και μόνο αν κάθε παράγοντας

$$\frac{p_j^{\alpha_j+1} - 1}{p_j - 1} = p_j^{\alpha_j} + p_j^{\alpha_j - 1} + \ldots + p_j + 1$$

είναι περιττός. Αν $p_1 = 2$ τότε πάντα ο $p_1^{\alpha_1} + p_1^{\alpha_1 - 1} + \ldots + p_1 + 1$ είναι περιττός. Επιπλέον για κάθε περιττό p_j το άθροισμα $p_j^{\alpha_j} + p_j^{\alpha_j - 1} + \ldots + p_j + 1$ είναι περιττός αν και μόνο αν ο εκθέτης α_j είναι άρτιος.
Επομένως, ο αριθμός $\sigma(\alpha)$ είναι περιττός αν και μόνο αν ο α είναι της μορφής $\alpha = 2^{\varkappa} \nu^2$, όπου ο $\varkappa$ είναι τυχαίος φυσικός και ο ν είναι περιττός.

30. Έστω $\delta = (2^{\nu} - 1, 2^{\mu} + 1)$ και $2^{\nu} - 1 = \varkappa\delta$ και $2^{\mu} + 1 = \lambda\delta$.
Έχουμε $2^{\mu\nu} = (\varkappa\delta + 1)^{\mu} = A\delta + 1$ και $2^{\mu\nu} = (\lambda\delta - 1)^{\nu} = B\delta - 1$, αφού ο ν είναι περιττός.
Έτσι $(B - A)\delta = 2$ άρα ο δ διαιρεί τον 2. Όμως προφανώς ο δ είναι περιττός, οπότε $\delta = 1$.

31. Προφανώς πρέπει $\mu > 3$. Έχουμε

$$\lambda^2 = \varkappa^{\mu} - \varkappa^3 = \varkappa^3(\varkappa^{\mu-3} - 1),$$

οπότε $\varkappa \mid \lambda$. Θέτουμε $\lambda = \varkappa\alpha$ οπότε $\alpha^2 = \varkappa(\varkappa^{\mu-3} - 1)$, δηλαδή ο αριθμός $\varkappa(\varkappa^{\mu-3} - 1)$ είναι τέλειο τετράγωνο.
Όμως, επειδή $\varkappa^{\mu-4}(\varkappa) - 1(\varkappa^{\mu-3} - 1) = 1$, οι αριθμοί $\varkappa$ και $\varkappa^{\mu-3}$ είναι πρώτοι μεταξύ τους, άρα καθένας από αυτούς είναι επίσης τέλειο τετράγωνο, δηλαδή $\varkappa = \beta^2$.
Έτσι έχουμε

$$\alpha^2 = \beta^2(\beta^{2(\mu-3)} - 1)$$

άρα ο β διαιρεί τον α και συνεπώς

$$-\left(\frac{\alpha}{\beta}\right)^2 + \beta^{2(\mu-3)} = 1$$

ή

$$\left(\beta^{\mu-3} - \frac{\alpha}{\beta}\right)\left(\beta^{\mu-3} + \frac{\alpha}{\beta}\right) = 1,$$

αδύνατο.

32. (α) Έστω $\alpha = 4\varkappa + 1$, $\beta = 4\lambda + 1$. Τότε $\alpha\beta = 4(4\varkappa\lambda + \varkappa + \lambda) + 1$, δηλαδή $\alpha\beta \in H$.

(β) Εάν ο $\nu \in H$ δεν είναι πρώτος, τότε από τον ορισμό θα έχουμε $\nu = \alpha\beta$ με $\alpha, \beta \in H$ και $\alpha, \beta > 1$.
Στη συνέχεια κάνουμε το ίδιο για καθένα από τους νέους παράγοντες. Η διαδικασία σταματά αφού σε κάθε βήμα παίρνουμε μικρότερους αριθμούς του Η, το οποίο έχει ελάχιστο στοιχείο το 1. Η ανάλυση δεν είναι μοναδική, αφού π.χ. $693 = 9 \cdot 77 = 21 \cdot 33$.

Λύσεις Ασκήσεων § 2.1

Α' Ομάδα

1. Η ισοτιμία $x^2 \equiv x(\mathrm{mod} p^\kappa)$ γράφεται $x(x-1) \equiv 0(mod p^\kappa)$.
   Άρα
   $$\begin{array}{lll} p^\kappa \mid x & \kappa\alpha\iota & x \equiv 0(mod p^\kappa) \quad \acute{\eta} \\ p^\kappa \mid x-1 & \kappa\alpha\iota & x \equiv 1(mod p^\kappa). \end{array}$$

2. Διακρίνουμε περιπτώσεις:

   - Αν $\nu \equiv 0(mod 10)$, τότε $\nu^2 \equiv 0(mod 10)$
   - Αν $\nu \equiv 1(mod 10)$, τότε $\nu^2 \equiv 1(mod 10)$
     $\vdots$
   - Αν $\nu \equiv 9(mod 10)$, τότε $\nu^2 \equiv 81 \equiv 1(mod 10)$.

3. (i) Έχουμε ότι
   $$\begin{array}{ll} & 145 \equiv 2(mod 13) \\ \acute{\eta} & 145^6 \equiv 2^6 \equiv -1(mod 13) \\ \acute{\eta} & 145^6 + 1 \equiv 0(mod 13). \end{array}$$
   Ανάλογα αντιμετωπίζουμε και τις υπόλοιπες περιπτώσεις.

4. Διακρίνουμε περιπτώσεις:
   $$\text{αν } \nu \equiv 1(mod 7) \text{ ,τότε } \nu^6 \equiv 1(mod 7)$$
   $$\text{αν } \nu \equiv 2(mod 7) \text{ ,τότε } \nu^6 \equiv 1(mod 7)$$
   $\vdots$
   $$\text{αν } \nu \equiv 6(mod 7) \text{ ,τότε } \nu^6 \equiv 36 \equiv 1(mod 7).$$
   Όμοια εργαζόμαστε και για την άλλη περίπτωση

5. Προφανής, αφού στο διώνυμο του Νέυτωνα:
   $(\nu+\mu)^p = \nu^p + \binom{p}{1} \nu^{p-1}\mu + \ldots + \mu^p$, όλοι οι όροι εκτός από τους ν^p και μ^p έχουν πρώτο παράγοντα τον p.

6. Αρκεί να υπολογίσουμε το $2^{10000}(mod 1000)$. Έχουμε ότι:

$$\begin{aligned}
2^{10} &\equiv 1024 \equiv 24(mod 1000) && \text{ή} \\
2^{20} &\equiv 576(mod 1000) && \text{ή} \\
2^{40} &\equiv 331776 \equiv 776(mod 1000) && \text{ή} \\
2^{60} &\equiv 446976 \equiv 976(mod 1000) && \text{ή} \\
2^{100} &\equiv 757376 \equiv 376(mod 1000) && \text{ή} \\
&\vdots && \vdots \\
2^{4000} &\equiv 141376 \equiv 376(mod 1000) && \text{ή} \\
2^{8000} &\equiv 141376 \equiv 376(mod 1000)
\end{aligned}$$

Άρα $2^{10000} = 2^{8000} \cdot 2^{2000} \equiv 376^2 \equiv 141376 \equiv 376(mod 1000)$ και τα τρία τελευταία ψηφία του $2^{10.000}$ είναι 376.

7. Παρατηρούμε ότι $9 \equiv 1(mod 8)$ και $17 \equiv 1(mod 8)$ και επομένως $9^{1998} \equiv 1(mod 8)$ και $17^{1999} \equiv 1(mod 8)$.
Άρα $9^{1998} + 17^{1999} \equiv 2(mod 8)$ και το υπόλοιπο της διαίρεσης του N διά του 8 είναι ίσο με 2.

8. Αφού ο ν είναι σύνθετος τότε $\nu = \alpha\beta$, για κάποιους φυσικούς α, β, με $1 < \alpha, \beta < \nu$.
Οι α, β θα εμφανίζονται ως όροι του παραγοντικού $(\nu - 1)!$, οπότε

$$(\nu - 1)! \equiv 0(mod \nu),$$

εκτός εάν ο ν είναι τετράγωνο πρώτου, δηλαδή $\nu = p^2$, όπου p περιττός πρώτος και ισχύει προφανώς και στην περίπτωση αυτή.

9. Έστω υ_1 το υπόλοιπο της διαίρεσης του α με τον ν και υ_2 το υπόλοιπο της διαίρεσης του β με τον ν, με $0 \leq \upsilon_1, \upsilon_2 \leq \nu$. Από τον ορισμό των ισοϋπόλοιπων αριθμών πρέπει $\upsilon_1 = \upsilon_2$, οπότε ισχύει ότι:

$$(\alpha, \nu) = (\upsilon_1, \nu) = (\upsilon_2, \nu) = (\beta, \nu).$$

10. Έχουμε διαδοχικά

$$\begin{aligned}
\mu &\equiv (-1) mod(\mu + 1) && \text{ή} \\
\mu^{2\nu} &\equiv (-1)^{2\nu} mod(\mu + 1) && \text{ή} \\
\mu^{2\nu} &\equiv 1 mod(\mu + 1).
\end{aligned}$$

Β' Ομάδα

11. Χρησιμοποιώντας τις ιδιότητες των ισοτιμιών έχουμε διαδοχικά:

$$5^{2\nu} \equiv 25^{\nu} \equiv 4^{\nu}(mod 7)$$
$$3 \cdot 2^{5\nu} \equiv 3 \cdot 32^{\nu} \equiv 3 \cdot 4^{\nu}(mod 7)$$
$$3 \cdot 2^{5\nu-2} \equiv 3 \cdot 4^{\nu-1}(mod 7),$$

αφού (2,7)=1 (ιδιότητα διαγραφής).
Επομένως

$$5^{2\nu} + 3 \cdot 2^{5\nu-2} \equiv 4^{\nu} + 3 \cdot 4^{\nu-1} \equiv 4^{\nu-1}(4+3) \equiv 4^{\nu-1} \cdot 7 \equiv 0(mod 7).$$

12. (i) Αλη*θ*ής
(ii) Αληθής
(iii) Ψευδής
(iv) Αληθής
(v) Αληθής
(vi) Αληθής
(vii) Ψευδής
(viii) Ψευδής

13. Ο x έχει αντίστροφο τον εαυτό του αν και μόνο αν

$$x^2 \equiv 1(mod p) \quad \text{ή}$$
$$x^2 - 1 \equiv 0(mod p) \quad \text{ή}$$
$$p \mid (x-1)(x+1)$$

και επειδή ο p είναι πρώτος, αυτό συμβαίνει αν και μόνο αν
$p \mid (x-1)$ ή $p \mid (x+1)$, δηλαδή $x \equiv 1(mod p)$ ή $x \equiv -1(mod p)$.

14. (α) Αν $p = 3$ τότε $8p - 1 = 25$ δηλαδή σύνθετος.
Αν $p \neq 3$ τότε $p \equiv 1$ ή $2(mod 3)$, όμως για $p \equiv 2(mod 3)$ έχουμε $8p - 1 \equiv 0(mod 3)$, δηλαδή $8p - 1$ σύνθετος.
Μένει να εξετάσουμε την περίπτωση $p \equiv 1(mod 3)$. Τότε όμως $8p + 1 \equiv 0(mod 3)$, δηλαδή σύνθετος.

(β) Αν $p \neq 3$ τότε $p \equiv 1$ ή $2(mod3)$, οπότε $p^2 \equiv 1(mod3)$ άρα $8p^2 + 1 \equiv 0(mod3)$, δηλαδή σύνθετος.
Η μόνη περίπτωση που ισχύει η υπόθεση είναι συνεπώς $p = 3$. Τότε όμως $8p^2 - 1 = 71$, δηλαδή πρώτος.

15. Η διακρίνουσα της εξίσωσης είναι $\Delta = \beta^2 - 4\alpha\gamma$.
Η εξίσωση έχει ρητές λύσεις αν και μόνο αν η διακρίνουσα είναι τέλειο τετράγωνο. Όμως αφού α, β, γ περιττοί,

$$\begin{aligned}\Delta &= \beta^2 - 4\alpha\gamma \\ &= (2\beta_1 + 1)^2 - 4(2\alpha_1 + 1)(2\gamma_1 + 1) \\ &= 4\beta_1(\beta_1 + 1) + 1 - 16\alpha_1\gamma_1 - 8\alpha_1 - 8\gamma_1 - 4 \\ &\equiv 5(mod8)\end{aligned}$$

άρα η διακρίνουσα δεν είναι τέλειο τετράγωνο, αφού κάθε τέλειο τετράγωνο είναι ισότιμο με 0, 1 ή $4(mod8)$.

16. (α) Αναζητούμε τους φυσικούς για τους οποίους $2^\nu \equiv 1(mod7)$.
Έχουμε $2^1 \equiv 2(mod7)$, $2^2 \equiv 4(mod7)$, $2^3 \equiv 1(mod7)$, άρα διακρίνουμε τις περιπτώσεις:

- $\nu = 3x$ $\quad 2^\nu \equiv 2^{3x} \equiv 1(mod7)$
- $\nu = 3x + 1$ $\quad 2^\nu \equiv 2^{3x+1} \equiv 2(mod7)$
- $\nu = 3x + 2$ $\quad 2^\nu \equiv 2^{3x+2} \equiv 4(mod7)$

έτσι οι ζητούμενοι φυσικοί είναι όλα τα πολλαπλάσια του 3.

(β) Χρησιμοποιώντας τις ίδιες περιπτώσεις με το (α) καταλήγουμε ότι

$$2^\nu + 1 \equiv 2 \text{ ή } 3 \text{ ή } 5(mod7).$$

17. Παρατηρούμε ότι αν x άρτιος τότε

$$x^4 = (2x)^4 \equiv 0(mod16)$$

ενώ αν x περιττός τότε

$$x^4 = (2x + 1)^4 = 8x(x + 1) + 1 \equiv 1(mod16).$$

Έτσι έχουμε $x_1^4 + x_2^4 + \ldots + x_{14}^4 \equiv 0$ ή 1 ή $2 \ldots$ ή $14(mod16)$.
Και επειδή $15999 \equiv 15(mod16)$, η εξίσωση είναι αδύνατη.

18. Διακρίνοντας περιπτώσεις για τον $\nu(mod4)$ και τον $\nu(mod9)$, για κάθε φυσικό αριθμό ν έχουμε ότι

$$\nu^2 \equiv 0 \text{ ή } 1(mod4) \qquad \text{και}$$
$$\nu^3 \equiv 0 \text{ ή } 1 \text{ ή } -1(mod9).$$

Άρα μια ακολουθία που ικανοποιεί την υπόθεση είναι η

$$\alpha_\nu = 36\nu + 3, \quad \nu = 1, 2, 3, \ldots.$$

19. (i) $0 + 100(mod24) \equiv 4(mod24)$. Θα είναι 4 το πρωί.
(ii) $15 + 1000(mod24) \equiv 7(mod24)$. Θα είναι 7 το πρωί.
(iii) $5 - 1000(mod24) \equiv 11(mod24)$. Θα είναι 11 το πρωί.

20. Για $\nu = 0$ ισχύει, αφού $4^0 = 1 \equiv 1(mod9)$.
Υποθέτουμε ότι ισχύει για $\nu = \kappa$, δηλαδή $4^\kappa \equiv 1 + 3\kappa(mod9)$.
Για $\nu = \kappa + 1$ έχουμε

$$\begin{aligned} 4^{\kappa+1} = 4 \cdot 4^\kappa &\equiv 4(1 + 3\kappa)(mod9) \\ &\equiv 4 + 3\kappa + 9\kappa(mod9) \\ &\equiv 4 + 3\kappa(mod9) \\ &\equiv 1 + 3(\kappa + 1)(mod9), \end{aligned}$$

οπότε η επαγωγή ολοκληρώθηκε.

Λύσεις Ασκήσεων § 2.2

Α' Ομάδα

1. (i) $15x \equiv 24(mod35)$.
Επειδή (15,35)=5 και $5 \not| 24$, η ισοτιμία δεν έχει λύση.

(ii) $20x \equiv 30(mod4)$ ή $20x \equiv 2(mod4)$.
Παρατηρούμε ότι ο 20 είναι πολλαπλάσιο του 4,οπότε για κάθε ακέραιο x ισχύει $20x \equiv 0(mod4)$.
Άρα η ισοτιμία είναι αδύνατη.

(iii) $353x \equiv 254(mod400)$ και (353,400)=1.
Από τον αλγόριθμο του Ευκλείδη,

$$\begin{aligned} 400 &= 353 + 47 \\ 353 &= 7 \cdot 47 + 24 \\ 47 &= 24 + 23 \\ 24 &= 23 + 1, \end{aligned}$$

οπότε

$$\begin{aligned} 1 &= 24 - 23 \\ &= 24(47 - 24) = 2 \cdot 24 - 47 \\ &= 2(353 - 7 \cdot 47) - 47 = 2 \cdot 353 - 15 \cdot 47 \\ &= 2 \cdot 353 - 15(400 - 353) = 17 \cdot 353 - 15 \cdot 400. \end{aligned}$$

Επομένως $17 \cdot 353 \equiv 1(mod400)$, άρα

$$\begin{aligned} 353x &\equiv 254(mod400) \quad \text{ή} \\ 17 \cdot 353x &\equiv 17 \cdot 254(mod400) \quad \text{ή} \\ x &\equiv 318(mod400). \end{aligned}$$

2. (i)
$$\left\{ \begin{array}{l} x \equiv 1(mod5) \\ x \equiv 3(mod7) \\ x \equiv 5(mod2) \end{array} \right\} \text{ ή } \left\{ \begin{array}{l} x \equiv 1(mod5) \\ x \equiv 3(mod7) \\ x \equiv 1(mod2) \end{array} \right\}$$
Επειδή οι αριθμοί 2,5,7 είναι πρώτοι μεταξύ τους, το σύστημα θα έχει μοναδική λύση $mod(2 \cdot 5 \cdot 7) = mod70$.

(ii) Όμοια με το (i).

Β' Ομάδα

3. Όμοια με την προηγούμενη άσκηση.

4. Οι ζητούμενοι αριθμοί είναι οι λύσεις του συστήματος

$$\left\{ \begin{array}{l} x \equiv 1(mod 2) \\ x \equiv 2(mod 3) \\ x \equiv 3(mod 5) \end{array} \right\},$$

το οποίο έχει λύση $x \equiv 23(mod 30)$.

5. Όμοια με τηην απόδειξη του Θεωρήματος 2.2.1.

6. Απλή εφαρμογή του Κινέζικου Θεωρήματος.

7. Έστω $\nu-10, \nu-9, \ldots, \nu+10$ οι ζητούμενοι αριθμοί. Παρατηρούμε ότι αν ο αριθμός ν διαιρείται με το $2 \cdot 3 \cdot 5 \cdot 7 = 210$, τότε όλοι οι αριθμοί εκτός από τους $\nu - 1$ και $\nu + 1$ θα έχουν κάποιον πρώτο παράγοντα $p \leq 7$. Αυτό συμβαίνει γιατί οι $\nu \pm 2$, $\nu \pm 4$, $\nu \pm 6, \ldots$ θα είναι πολλαπλάσια του 2, οι $\nu \pm 3$, $\nu \pm 6$, $\nu \pm 9, \ldots$ θα είναι πολλαπλάσια του 3 κ.λπ.
Αρκεί να προσδιορίσουμε τον ν για τον οποίο οι $\nu - 1$ και $\nu + 1$ διαιρούνται με το 11 ή το 13. Αρκεί να λύσουμε το σύστημα

$$\nu \equiv 0(mod 210), \;\; \nu \equiv 1(mod 11), \;\; \nu \equiv -1(mod 13).$$

(Δεν είναι δυνατόν οι $\nu + 1$, $\nu - 1$ να διαιρούνται και οι δύο με το 11 ή το 13 αφού διαφέρουν κατά 2.)
Από το Κινέζικο Θεώρημα γνωρίζουμε ότι υπάρχουν άπειροι τέτοιοι ν. Για παράδειγμα ο $\nu = 9450$ δίνει τους 21 αριθμούς 9449, 9441,...,9460.

Λύσεις Ασκήσεων § 2.3

Α' Ομάδα

1. Έχουμε $\varphi(3600) = \varphi(2^4 \cdot 3^2 \cdot 5^2) = 960$ τέτοιους αριθμούς, λόγω του Πορίσματος 2.3.4.

2. Έχουμε $100 = 2^5 \cdot 5^2$, άρα από το Πόρισμα 2.3.4

$$\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100\left(\frac{1}{2}\right)\left(\frac{4}{5}\right) = 40$$

Όμοια βρίσκουμε $\varphi(1000)=400$ και $\varphi(7200)=1920$.

3. Προφανής, από τον τύπο του Πορίσματος 2.3.4.

4. Είναι άμεση από το Πόρισμα 2.3.4.

Β' Ομάδα

5. Έστω ένας φυσικός ν, τέτοιος ώστε $\varphi(2\nu)=\varphi(\nu)$.
Από το Πόρισμα 2.3.4 έχουμε :

(i) Αν ν άρτιος, τότε

$$2\nu\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{p_2}\right)\ldots\left(1 - \tfrac{1}{p_\kappa}\right) = \nu\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{p_2}\right)\ldots\left(1 - \tfrac{1}{p_\kappa}\right)$$

δηλαδή $2\nu=\nu$, άτοπο.

(ii)Αν ν περιττός ,τότε

$$2\nu\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{p_1}\right)\ldots\left(1 - \tfrac{1}{p_\kappa}\right) = \nu\left(1 - \tfrac{1}{p_1}\right)\ldots\left(1 - \tfrac{1}{p_\kappa}\right)$$

με $p_1 < 2$, δηλαδή $\nu = \nu$ το οποίο ισχύει.
Άρα $\varphi(2\nu)=\varphi(\nu)$ αν και μόνο αν ο φυσικός ν είναι περιττός.

6. Έστω ν ένας φυσικός αριθμός με κ διαφορετικούς περιττούς πρώτους παράγοντες $p_1, p_2, \ldots p_\kappa$.
Από το Πόρισμα 2.3.4 έχουμε

$$\varphi(\nu) = \nu\left(1 - \tfrac{1}{p_1}\right)\left(1 - \tfrac{1}{p_2}\right)\ldots\left(1 - \tfrac{1}{p_\kappa}\right) \quad \acute{\eta}$$

$$\varphi(\nu) = \nu \cdot \frac{(p_1-1)(p_2-1)\ldots(p_\kappa-1)}{p_1 \cdot p_2 \cdot \ldots \cdot p_\kappa} \quad \acute{\eta}$$

$$\varphi(\nu) = (p_1 - 1)(p_2 - 1)\ldots(p_\kappa - 1)$$

όπου κάθε παράγοντας είναι άρτιος.
Δηλαδή για κάθε $j = 1, 2, \ldots, \kappa$ ισχύει $2 \mid (p_j - 1)$, άρα $2^\kappa \mid \varphi(\nu)$.

7. Η εξίσωση φ(ν)=24 γράφεται

$$\nu\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\ldots\left(1-\tfrac{1}{p_\kappa}\right) = 24 \quad \acute{\eta}$$

$$\tfrac{\nu\cdot(p_1-1)(p_2-1)\ldots(p_\kappa-1)}{p_1 p_2 \ldots p_\kappa} = 2^3 \cdot 3 \quad \acute{\eta}$$

$$\tfrac{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}(p_1-1)(p_2-1)\ldots(p_\kappa-1)}{p_1 p_2 \ldots p_\kappa} = 2^3 \cdot 3$$

όπου $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ είναι η κανονική μορφή του φυσικού ν.
Προφανώς κ=2 και

$$p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} (p_1 - 1)(p_2 - 1) = 2^3 \cdot 3 \quad \acute{\eta}$$

$$2^{\alpha_1 - 1} 3^{\alpha_2 - 1} (2 - 1)(3 - 1) = 2^3 \cdot 3 \quad \acute{\eta}$$

$$2^{\alpha_1} \cdot 3^{\alpha_2 - 1} = 2^3 \cdot 3.$$

Άρα $\alpha_1 = 3$ και $\alpha_2 = 2$, δηλαδή $\nu = 2^3 \cdot 3^2 = 72$.

8. Έστω φυσικός ν τέτοιος ώστε

$$\varphi(\nu) = 14 \quad \acute{\eta}$$

$$\nu\left(1-\tfrac{1}{p_1}\right)\left(1-\tfrac{1}{p_2}\right)\ldots\left(1-\tfrac{1}{p_\kappa}\right) = 2 \cdot 7 \quad \acute{\eta}$$

$$p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_\kappa^{\alpha_\kappa - 1} (p_1 - 1)(p_2 - 1)\ldots(p_\kappa - 1) = 2 \cdot 7.$$

όπου $\nu = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_\kappa^{\alpha_\kappa}$ είναι η κανονική μορφή του ν.
Η παραπάνω σχέση είναι προφανώς αδύνατη, άρα δεν υπάρχει τέτοιος φυσικός ν.

9. Έστω ν και κ δύο φυσικοί αριθμοί με αντίστοιχες κανονικές μορφές
$\nu = p_1^{a_1} p_2^{a_2} \ldots p_\tau^{a_\tau}$ και $\nu = q_1^{b_1} q_2^{b_2} \ldots q_\iota^{b_\iota}$.

Από το Πόρισμα 2.3.4 έχουμε

$$\varphi(x) = \varphi(\nu \cdot x) \qquad \text{ή}$$

$$x \cdot \left(1 - \tfrac{1}{q_1}\right)\left(1 - \tfrac{1}{q_2}\right) \ldots \left(1 - \tfrac{1}{q_t}\right) = \\ = \nu \cdot x \cdot \left(1 - \tfrac{1}{p_1}\right) \ldots \left(1 - \tfrac{1}{p_\tau}\right) \ldots \left(1 - \tfrac{1}{q_t}\right) \qquad \text{ή}$$

$$1 = \nu^{\frac{(1-p_1)(1-p_2)\ldots(1-p_\tau)}{p_1 p_2 \cdots p_\tau}} \qquad \text{ή}$$

$$p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \ldots p_\tau^{\alpha_\tau - 1} \cdot (1 - p_1)(1 - p_2) \ldots (1 - p_\tau) = 1.$$

Η τελευταία σχέση ισχύει μόνο αν τ=1, $p_1 = 2$ και $\alpha_1 = 1$. Δηλαδή, $\nu = 2$ και ο x είναι περιττός.

10. Από το Θεώρημα 2.3.2 και το Πόρισμα 2.3.4 έχουμε:

$$\begin{aligned} \varphi(1) &= 1 \\ \varphi(p) &= p - 1 \\ \varphi(p^2) &= p^2\left(1 - \tfrac{1}{p}\right) = p(p-1) = p^2 - p \\ &\vdots \\ \varphi(p^x) &= p^x\left(1 - \tfrac{1}{p}\right) = p^{x-1}(p-1) = p^x - p^{x-1}. \end{aligned}$$

Άρα

$$\begin{aligned} \varphi(1) + \varphi(p) + \ldots + \varphi(p^x) &= 1 + p - 1 + \ldots + p^x - p^{x-1} \\ &= p^x. \end{aligned}$$

Λύσεις Ασκήσεων § 2.4

Α' Ομάδα

1. Για $\kappa = 1$ έχουμε $\nu^2 \equiv 1(mod 8)$, που ισχύει.
   Έστω ότι η σχέση ισχύει για $\kappa \geq 1$, δηλαδή
   $\nu^{2^\kappa} \equiv 1 mod(2^{\kappa+2})$ ή $\nu^{2^\kappa} \equiv \mu \cdot 2^{\kappa+2} + 1$, για κάποιον μ.
   Είναι

$$\begin{aligned} \nu^{2^{\kappa+1}} = (\nu^{2^\kappa})^2 = (\mu \cdot 2^{\kappa+2} + 1)^2 &= \mu^2 \cdot 2^{2\kappa+4} + \mu \cdot 2^{\kappa+3} + 1 \\ &\equiv 0 + 0 + 1(mod 2^{\kappa+3}). \end{aligned}$$

   Οπότε η σχέση ισχύει για κάθε $\kappa \geq 1$.

2. Είναι $\nu^{p\delta} - 1 = (\nu^\delta - 1)(\nu^{\delta(p-1)} + \nu^{\delta(p-2)} + \ldots + \nu^\delta + 1)$.
   Αλλά $p^\mu \mid (\nu^\delta - 1)$ και

$$\begin{aligned} \nu^{\delta(p-1)} + \nu^{\delta(p-2)} + \ldots + \nu^\delta + 1 &\equiv 1^{p-1} + 1^{p-2} + \ldots + 1^2 + 1 + 1 \\ &\equiv p \equiv 0(mod p). \end{aligned}$$

   (Αν $\nu^\delta \equiv 1(mod p^\mu)$, τότε $\nu^\delta \equiv 1(mod p)$).
   Οπότε $p \mid \nu^{\delta(p-1)} + \nu^{\delta(p-2)} + \ldots + \nu^\delta + 1$, άρα

$$p^{\mu+1} \mid (\nu^{p\delta} - 1) \text{ και } \nu^{p\delta} \equiv 1(mod p^{\mu+1}).$$

3. Άμεση εφαρμογή του θεωρήματος Fermat. (Για την περίπτωση $\nu^9 - \nu$ έχουμε $2^9 - 2 = 510$ που δε διαιρείται με το 9).

4. Αρκεί να αποδείξουμε ότι ο αριθμός αυτός διαιρείται με τους αριθμούς $2, 3, 5, 7, 11, 13, 31, 61$.
   Για τη διαίρεση με το 2 παρατηρούμε ότι αν ένας από τους μ, ν είναι άρτιος τότε ο $\mu\nu$ διαιρείται με το 2 ενώ αν οι μ, ν είναι περιττοί ο $\mu^{60} - \nu^{60}$ είναι άρτιος ως διαφορά δύο περιττών.
   Για τη διαίρεση με τους υπόλοπους αριθμούς χρησιμοποιούμε το Θεώρημα Fermat. Έστω ότι θέλουμε να εξετάσουμε την περίπτωση $p = 7$. Αν ένας από τους μ, ν είναι πολλαπλάσιο του 7 τότε ο $\mu\nu$ διαιρείται με το 7. Διαφορετικά $(\mu, 7) = (\nu, 7) = 1$, οπότε έχουμε

$$\begin{aligned} \mu^{p-1} &\equiv \nu^{p-1} \equiv 1(mod 7) \quad \text{ή} \\ \mu^6 &\equiv \nu^6 \equiv 1(mod 7), \quad \text{άρα} \\ \mu^{60} &\equiv \nu^{60} \equiv 1(mod 7) \end{aligned}$$

δηλαδή ο 7 διαιρεί τον $\mu^{60} - \nu^{60}$.
Όμοια εργαζόμαστε και στις άλλες περιπτώσεις παρατηρώντας ότι το 60 είναι πολλαπλάσιο των αριθμών $2, 4, 6, 10, 12, 30, 60$.

5. Για $\nu = 1$ προφανώς ισχύει. Για $\nu \geq 2$ έχουμε ότι $91 = 7 \cdot 13$, οπότε αρκεί να δείξουμε ότι οι 7,13 διαιρούν το $\nu^{37} - \nu$. Από το Θεώρημα Fermat γνωρίζουμε ότι για $(\nu, 7) =$, ισχύει:

$$\begin{aligned} \nu^6 &\equiv 1(mod7) \text{ άρα} \\ \nu^{36} &\equiv 1(mod7) \text{ άρα} \\ \nu^{37} &\equiv \nu(mod7). \end{aligned}$$

Η τελευταία σχέση ισχύει και στην περίπτωση που $(\nu, 7) > 1$ αφού τότε $\nu^{37} \equiv \nu \equiv 0(mod7)$ δηλαδή πάντοτε $7 \mid (\nu^{37} - \nu)$. Όμοια αποδεικνύουμε ότι $13 \mid (\nu^{37} - \nu)$.

Β' Ομάδα

6. Θα δώσουμε έναν τρόπο κατασκευής ακεραίων της μορφής $\alpha_i = 2^{x_i} - 3,\ i = 1, 2, 3, \ldots$ οι οποίες ανά δύο είναι πρώτοι μεταξύ τους. Έστω ότι έχουμε $\nu \geq 2$ σχετικά πρώτους αριθμούς

$$\alpha_1 = 2^{x_1} - 3,\ \ \alpha_2 = 2^{x_2} - 3, \ldots,\ \ \alpha_\nu = 2^{x_\nu} - 3.$$

Θεωρούμε το γινόμενο $\Gamma = \alpha_1\alpha_2 \ldots \alpha_\nu$, το οποίο είναι περιττός αριθμός ως γινόμενο περιττών άρα $(\Gamma, 2) = 1$. Από το Θεώρημα Euler θα υπάρχει ακέραιος $\beta \geq 1$ τέτοιος ώστε $2^\beta \equiv 1(mod\Gamma)$, δηλαδή ο Γ διαιρεί τον $2^\beta - 1$. Επειδή ο Γ είναι περιττός, θα είναι σχετικά πρώτος με τον $(2^\beta - 1) - 2 = 2^\beta - 3$, αφού διαφορετικά αν υπήρχε κοινός διαιρέτης $p > 1$ τότε ο p θα διαιρούσε τους $2^\beta - 1$ και $2^\beta - 3$ άρα και τον 2, δηλαδή $p = 2$ αδύνατο αφού Γ περιττός. Ο αριθμός $2^\beta - 3$ είναι της κατάλληλης μορφής και είναι σχετικά πρώτος με τους $\alpha_1, \ldots, \alpha_\nu$ αφού είναι σχετικά πρώτος με το γινόμενό τους. Με αυτή τη διαδικασία μπορούμε να κατασκευάσουμε άπειρους ακεραίους αυτής της μορφής, ξεκινώντας από δύο αριθμούς, τους α_1 και α_2. Αρκεί να αποδείξουμε ότι δύο τέτοιοι αριθμοί υπάρχουν. Πράγματι, μπορούμε να ξεκινήσουμε π.χ. με $\alpha_1 = 5$ και $\alpha_2 = 13$.

7. Επειδή p, q πρώτοι έχουμε $(p, q) = 1$ άρα από το Θεώρημα Fermat,

$$p^{q-1} \equiv 1(modq) \text{ και } q^{p-1} \equiv 1(modp)$$

δηλαδή

$$q \mid (p^{q-1} - 1) \text{ και } p \mid (q^{p-1} - 1)$$

άρα

$$pq \mid (p^{q-1} - 1)(q^{p-1} - 1) \text{ ή } pq \mid (-p^{q-1} - q^{p-1} + 1)$$

άρα $p^{q-1} + q^{p-1} \equiv 1(modpq)$.

8. Εργαζόμαστε όπως στην περίπτωση που α, β είναι πρώτοι (προηγούμενη άσκηση).

9. Επειδή $(\alpha, \beta) = 1$, ο α θα είναι περιττός οπότε $\alpha^2 \equiv 1(mod8)$. Επίσης από το Θεώρημα Euler $\alpha^2 \equiv 1(mod6)$, αφού $\varphi(6) = 2$ άρα οι αριθμοί 6 και 8 διαιρούν τον $\alpha^2 - 1$ άρα και ο $[6, 8] = 24$ θα διαιρεί τον $\alpha^2 - 1$ οπότε $\alpha^2 \equiv 1(mod24)$.

10. Από το Θεώρημα Euler, $2^{\varphi(\nu)} \equiv 1(mod\nu)$. Όμως το $\nu!$ διαιρείται με το $\varphi(\nu)$, αφού το $\varphi(\nu)$ είναι ένας αριθμός μικρότερος του ν. Άρα $2^{\nu!} \equiv 1(mod\nu)$ που σημαίνει ότι ο αριθμός $(2^{\nu!} - 1)/\nu$ είναι ακέραιος.

Λύσεις Ασκήσεων του 2.5

Α' Ομάδα

1. Από το θεώρημα Wilson έχουμε ότι

$$\begin{aligned}(p-1)! &\equiv -1(mod p) \quad \acute{\eta}\\ (p-3)!(p-2)(p-1) &\equiv -1(mod p) \quad \acute{\eta}\\ (p-3)!(-2)(-1) &\equiv -1(mod p) \quad \acute{\eta}\\ (p-3)! &\equiv -1(mod p).\end{aligned}$$

2. Έχουμε ότι

$$\begin{aligned}(p-1)! &= (1\cdot 2\cdot 3\cdot \ldots \cdot \tfrac{p-1}{2})(\tfrac{p+1}{2}\cdot \ldots \cdot (p-1))\\ &\equiv (1\cdot 2\cdot 3\cdot \ldots \cdot \tfrac{p-1}{2})(\tfrac{p+1-2p}{2}\cdot \ldots \cdot (-1))(mod p)\\ &\equiv (1\cdot 2\cdot 3\cdot \ldots \cdot \tfrac{p-1}{2})^2(-1)^{\frac{(p-1)}{2}}(mod p)\end{aligned}$$

Επειδή $p \equiv 1(mod 4)$, ο $\frac{p-1}{2}$ είναι άρτιος, άρα
$[(\frac{p-1}{2})!]^2 \equiv (p-1)!(mod p) \equiv -1(mod p)$.

3. Όμοια με την προηγούμενη άσκηση.

Β' Ομάδα

4. Έστω ότι οι $(\gamma_1, \gamma_2, \ldots, \gamma_p)$ είναι μια τέτοια μετάθεση. Αν υποθέσουμε ότι $\alpha_i = 0$ και $\beta_j = 0$ για κάποιους i, j τότε $\gamma_i = \gamma_j = 0$ αδύνατο, αφού οι $\gamma_1, \gamma_2, \ldots, \gamma_p$ πρέπει να είναι όλοι διαφορετικοί μεταξύ τους. Έτσι πρέπει $i = j$. Υποθέτουμε χωρίς βλάβη της γενικότητας ότι $\alpha_p = \beta_p = 0$ οπότε $\gamma_p = 0$. Όμως έχουμε $(p-1)! \equiv \alpha_1\alpha_2\ldots\alpha_{p-1} \equiv \beta_1\beta_2\ldots\beta_{p-1}(mod p)$ άρα

$$\begin{aligned}[(p-1)!]^2 &\equiv (\alpha_1\alpha_2\ldots\alpha_{p-1})(\beta_1\beta_2\ldots\beta_{p-1})(mod p)\\ &\equiv (\gamma_1\gamma_2\ldots\gamma_{p-1})(mod p)\\ &\equiv (p-1)!(mod p),\end{aligned}$$

συνεπώς $(p-1)! \equiv 1(mod p)$, άτοπο αφού από το Θεώρημα Wilson ισχύει ότι $(p-1)! \equiv -1(mod p) \not\equiv 1(mod p)$ για $p > 2$.

5. Για $\nu = 2, 3$ με δοκιμή διαπιστώνουμε ότι το σύνολο $1!, \ldots, \nu!$ είναι το $0, \ldots, (\nu-1) mod \nu$.

Για $\nu > 3$ θα αποδείξουμε ότι κάτι τέτοιο είναι αδύνατο. Αν ο ν είναι πρώτος, τότε από το θεώρημα Wilson $(\nu-1)! \equiv -1(mod\nu)$, άρα $(\nu-2)! \equiv 1(mod\nu)$, οπότε υπάρχουν δύο στοιχεία του συνόλου ισότιμα με το $1(mod\nu)$, το $(\nu-2)!$ και το $1!$.
Αν ο ν είναι σύνθετος, δηλαδή $\nu = \kappa\lambda$ με $\kappa < \lambda$ τότε
$\lambda! = 1 \cdot 2 \cdot \ldots \cdot \kappa \cdot \ldots \cdot (\lambda-1) \cdot \lambda \equiv 0(mod\nu)$ και
$\nu! = \lambda! \cdot (\lambda+1) \cdot \ldots \cdot \nu \equiv 0(mod\nu)$. Απομένει η περίπτωση που $\nu = \kappa^2$.
Στην περίπτωση αυτή έχουμε επίσης $(2\kappa)! \equiv 0 \equiv \nu!(mod\nu)$.

Λύσεις Γενικών Ασκήσεων του 2ου Κεφαλαίου

1. Αν ο αριθμός διαιρείται με το 121 θα διαιρείται και με το 11. Όμως $\nu^2+3\nu+5=(\nu+7)(\nu-4)+33$, που σημαίνει ότι ο $(\nu+7)(\nu-4)$ διαιρείται με το 11.
   Όμως οι αριθμοί $\nu+7$ και $\nu-4$ είναι ισοϋπόλοιποι modulo 11 άρα πρέπει καθένας να είναι πολλαπλάσιο του 11. Έτσι έχουμε

$$(\nu+7)(\nu-4)+33\equiv 33(mod 121),$$

   δηλαδή ο αριθμός $\nu^2+3\nu+5$ δεν είναι πολλαπλάσιο του 121.

2. Έστω α το όριο της ακολουθίας. Από τη σχέση

$$(A_{\nu+1})^2=\varkappa+A_\nu$$

   προκύπτει ότι $\alpha^2=\varkappa+\alpha$ οπότε

$$\alpha=\frac{1}{2}(1+\sqrt{4\varkappa+1}),$$

   αφού $\alpha\geq 0$.
   Ο αριθμός α είναι ακέραιος αν και μόνο αν ο αριθμός $4\varkappa+1$ είναι τέλειο τετράγωνο περιττού, δηλαδή αν $\varkappa=\lambda^2+\lambda$, για κάποιον φυσικό $\lambda>0$, οπότε $\alpha=\lambda+1$.
   Εάν ο $\varkappa$ είναι περιττός, τότε ο αριθμός $4\varkappa+1$ είναι ισότιμος με $5(mod 8)$ οπότε αποκλείεται να είναι τέλειο τετράγωνο. Σε αυτή την περίπτωση ο α είναι άρρητος.

3. Έχουμε

$$2^x=7+3^y\equiv 1(mod 3)$$

   οπότε ο x πρέπει να είναι άρτιος, δηλαδή $x\geq 2$. Έτσι

$$3^y=2^x-7\equiv 1(mod 4),$$

   δηλαδή ο y πρέπει να είναι άρτιος.
   Θέτουμε $x=2\varkappa$, $y=2\lambda$ οπότε έχουμε

$$(2^\varkappa-3^\lambda)(2^\varkappa+3^\lambda)=7$$

και επειδή ο 7 είναι πρώτος πρέπει

$$2^x - 3^\lambda = 1 \text{ και } 2^x + 3^\lambda = 7,$$

αφού ο πρώτος παράγοντας είναι μικρότερος του δεύτερου.
Από αυτές τις σχέσεις παίρνουμε $2^x = 4$ και $3^\lambda = 3$ δηλαδή $x = 2$, $\lambda = 1$ άρα $x = 4$, $y = 2$.

4. Θα αποδείξουμε ότι κάθε αριθμός της μορφής $72x + 42$ δε μπορεί να γραφεί ως άθροισμα εννιά ή λιγότερων τετραγώνων περιττών.
'Εστω ότι

$$72x + 42 = x_1^2 + x_2^2 + \ldots + x_\mu^2$$

όπου $x \geq 0$ και $1 \leq \mu \leq 9$.
Επειδή οι x_i είναι περιττοί, θα έχουμε $x_i^2 \equiv 1(mod 8)$ οπότε πρέπει

$$72x + 42 \equiv \mu(mod 8) \text{ ή}$$

$$\mu \equiv 2(mod 8)$$

άρα $\mu = 2$.
'Ομοια modulo 3 έχουμε

$$72x + 42 \equiv x_1^2 + x_2^2 + \ldots + x_\mu^2(mod 3) \text{ ή}$$

$$x_1^2 + x_2^2 \equiv 0(mod 3)$$

και επειδή $x^2 \equiv 0$ ή $1(mod 3)$ για κάθε ακέραιο x θα πρέπει να έχουμε

$$x_1 \equiv x_2 \equiv 0(mod 3).$$

Τέλος δουλεύοντας modulo 9 παίρνουμε $72x+42 \equiv x_1^2+x_2^2(mod 9)$ ή $6 \equiv 0(mod 9)$, άτοπο.

5. Επειδή το πλήθος των κλάσεων ισοδυναμίας moduloβ είναι πεπερασμένο θα υπάρχουν φυσικοί i, j με $i < j$ τέτοιοι ώστε

$$3^j \equiv 3^i(mod\beta).$$

Τότε όμως ο β θα διαιρεί τον αριθμό

$$3^j - 3^i = 3^i(3^{j-i} - 1)$$

άρα και τον $3^{j-i}-1$, αφού $(\beta,3)=1$.
Έτσι έχουμε

$$\frac{\alpha}{\beta}=\frac{\alpha\frac{3^{j-i}-1}{\beta}}{\beta\frac{3^{j-i}-1}{\beta}}=\frac{\alpha(3^{j-i}-1)/\beta}{3^{j-i}-1}.$$

6. (i) Έχουμε ότι:

$$9\cdot 10+6\cdot 9+0\cdot 8+0\cdot 7+6\cdot 6+0\cdot 5+6\cdot 4+1\cdot 3+2\cdot 6+1\cdot 1=$$
$$=222\equiv 0(mod 11)$$
$$1\cdot 10+8\cdot 9+5\cdot 8+3\cdot 7+2\cdot 6+6\cdot 5+0\cdot 4+8\cdot 3+6\cdot 2+10\cdot 1=$$
$$=231\equiv 0(mod 11).$$

(ii) Ισχύει ότι:
(α) Έστω $\alpha_{10}\alpha_9\ldots\alpha_1$ ο σωστός ISBN και αλλάζουμε το j-οστό ψηφίο του από α_j σε α_j'.
Επειδή

$$\sum_{x=1}^{10}x\alpha_x\equiv 0(mod 11)$$

έχουμε

$$j\cdot\alpha_j\equiv-\sum_{x\neq j}x\alpha_j(mod 11).$$

Άρα

$$\begin{aligned}10\alpha_{10}+\ & 9\alpha_9+\ldots+(j+1)\alpha_{j+1}+j\alpha_j'+(j-1)\alpha_{j-1}+\ldots+\alpha_1\equiv\\ &\equiv j\alpha_j'-j\alpha_j(mod 11)\\ &\equiv j(\alpha_j'-\alpha_j)(mod 11)\\ &\not\equiv 0(mod 11),\end{aligned}$$

αφού οι αριθμοί j και $\alpha_j'-\alpha_j$ είναι μεγαλύτεροι του 0 και μικρότεροι του 11.

(β) Όμοια με το (α), αν αλλάξουμε τους διαφορετικούς αριθμούς α_j, α_{j+1} μεταξύ τους τότε

$$\begin{aligned}10\alpha_{10}+\ & \ldots+(j+1)\alpha_j+j\alpha_{j+1}+\ldots+\alpha_1\equiv\\ &\equiv(j+1)\alpha_j+j\alpha_{j+1}-(j+1)\alpha_{j+1}-j\alpha_j(mod 11)\\ &\equiv\alpha_j-\alpha_{j+1}(mod 11)\\ &\not\equiv 0(mod 11).\end{aligned}$$

7. Απόδειξη με επαγωγή:
   Για $\nu = 1$ έχουμε

$$\alpha^2 - 1 = 4\left(\frac{\alpha+1}{2}\right)\left(\frac{\alpha-1}{2}\right).$$

Ένας από τους αριθμούς $\frac{\alpha+1}{2}$ και $\frac{\alpha-1}{2}$ είναι περιττός και επειδή είναι και οι δύο μεγαλύτεροι του 1 θα έχει έναν περιττό πρώτο παράγοντα. Έτσι ο αριθμός α^2-1 έχει δύο διαφορετικούς πρώτους παράγοντες (ο άλλος είναι ο 2).
Υποθέτουμε ότι η υπόθεση ισχύει για κάποιο $\nu \geq 1$. Για $\nu+1$ έχουμε

$$\alpha^{2^{\nu+1}} - 1 = (\alpha^{2^\nu} + 1)(\alpha^{2^\nu} - 1).$$

Ο δεύτερος παράγοντας έχει $\nu+1$ διαφορετικούς πρώτους παράγοντες από την υπόθεση της επαγωγής ενώ ο πρώτος είναι ισότιμος με $2(mod 4)$, οπότε θα έχει έναν περιττό πρώτο παράγοντα.
Αυτός ο παράγοντας δε μπορεί να είναι κάποιος από τους παράγοντες του $\alpha^{2^\nu} - 1$, αφού τότε αυτός θα διαιρούσε και τη διαφορά τους, δηλαδή το 2, αδύνατο. Έτσι ο αριθμός $\alpha^{2^{\nu+1}} - 1$ έχει $\nu+2$ διαφορετικούς πρώτους παράγοντες και το ζητούμενο έχει αποδειχθεί.

8. Έστω $x = \frac{\alpha}{\beta}$ και $y = \frac{\gamma}{\delta}$ με $(\alpha,\beta) = (\gamma,\delta) = 1$ και $\beta, \delta > 0$.
   Έχουμε λοιπόν $\varepsilon\varphi\frac{\pi\alpha}{\beta} = \frac{\gamma}{\delta}$.
   Από το Θεώρημα De Moivre έχουμε:

$$\begin{aligned}
\left(\tfrac{\delta+i\gamma}{\delta-i\gamma}\right)^\beta &= \left(\tfrac{1+i\gamma/\delta}{1-i\gamma/\delta}\right)^\beta \\
&= \left(\tfrac{1+i\varepsilon\varphi(\pi\alpha/\beta)}{1-i\varepsilon\varphi(\pi\alpha/\beta)}\right)^\beta \\
&= \left(\tfrac{\sigma\upsilon\nu(\pi\alpha/\beta)+i\eta\mu(\pi\alpha/\beta)}{\sigma\upsilon\nu(\pi\alpha/\beta)-i\eta\mu(\pi\alpha/\beta)}\right)^\beta \\
&= \tfrac{\sigma\upsilon\nu(\pi\alpha/\beta)+i\eta\mu(\pi\alpha/\beta)}{\sigma\upsilon\nu(\pi\alpha/\beta)-i\eta\mu(\pi\alpha/\beta)} = 1,
\end{aligned}$$

δηλαδή

$$\begin{aligned}(\delta+i\gamma)^\beta &= (\delta-i\gamma)^\beta \\ &= ((\delta+i\gamma)-2i\gamma)^\beta \\ &= \textstyle\sum_{\varkappa=0}^{\beta}\binom{\beta}{\varkappa}(\delta+i\gamma)^{\beta-\varkappa}(-2i\gamma)^\varkappa\end{aligned}$$

άρα

$$\begin{aligned}(-2i\gamma)^\beta &= -\textstyle\sum_{\varkappa=1}^{\beta-1}\binom{\beta}{\varkappa}(\delta+i\gamma)^{\beta-\varkappa} \\ &= -(\delta+i\gamma)\textstyle\sum_{\varkappa=1}^{\beta-1}\binom{\beta}{\varkappa}(\delta+i\gamma)^{\beta-\varkappa-1} \\ &= (\delta+i\gamma)(x+iy).\end{aligned}$$

Παίρνοντας τα μέτρα των μιγαδικών στην τελευταία σχέση έχουμε

$$2^{2\beta}\gamma^{2\beta} = (\delta^2+\gamma^2)(x^2+y^2).$$

Έστω p ένας περιττός πρώτος παράγοντας του $\delta^2+\gamma^2$. Τότε ο p θα διαιρεί και τον $2^{2\beta}\gamma^{2\beta}$ άρα θα διαιρεί και τον γ, άρα θα διαιρεί και τον $(\delta^2+\gamma^2)-\gamma^2=\delta^2$, άτοπο αφού $(\gamma,\delta)=1$ από την υπόθεση. Συνεπώς ο $\delta^2+\gamma^2$ δεν έχει περιττούς πρώτους παράγοντες δηλαδή είναι μία δύναμη του 2.
Επειδή όμως $(\delta,\gamma)=1$, οι δ, γ δε μπορεί να είναι και οι δύο άρτιοι, άρα

$$\delta^2+\gamma^2=1 \text{ ή } \delta^2+\gamma^2=2.$$

Έτσι έχουμε τις περιπτώσεις

$$(\gamma,\delta)=(0,1) \text{ ή } (\gamma,\delta)=(\pm1,1).$$

Η πρώτη περίπτωση δίνει $x=\frac{\varkappa}{4}$ για κάποιον ακέραιο $\varkappa=4\lambda$ ενώ η δεύτερη $x=\frac{\varkappa}{4}$ για κάποιο $\varkappa\equiv 1(mod 2)$, δηλαδή γενικά $x=\frac{\varkappa}{4}$ με $\varkappa\equiv 0,1 \text{ ή } 3(mod 4)$.

9. Έστω $X=4444^{4444}$ για Γ το άθροισμα των ψηφίων του Β. Γνωρίζουμε ότι ένας αριθμός και άθροισμα των ψηφίων του είναι ισοϋπόλοιπος modulo9, δηλαδή

$$X\equiv A\equiv B\equiv \Gamma(mod 9).$$

Επίσης

$$\begin{aligned} 4444^{4444} &\equiv 7^{4444}(mod 9) \\ &\equiv 7^{3\cdot 1481}\cdot 7(mod 9) \\ &\equiv 7(mod 9), \end{aligned}$$

αφού $7^3 \equiv 1(mod 9)$.
Έτσι έχουμε $\Gamma \equiv 7(mod 9)$.
Θα βρούμε ένα πάνω όριο για το πλήθος των ψηφίων του X. Έχουμε

$$\log X = 4444 \log 4444 < 4444 \log 10^4 = 4444 \cdot 4 = 17776$$

όπου log ο δεκαδικός λογάριθμος.
Αν όμως ο δεκαδικός λογάριθμος ενός ακεραίου είναι μικρότερος ενός αριθμού ν τότε ο αριθμός έχει το πολύ ν ψηφία, δηλαδή ο X έχει το πολύ 17776 ψηφία.
Ακόμα και αν όλα τα ψηφία του ήταν 9, το άθροισμα των ψηφίων του X θα ήταν το πολύ $9 \cdot 17776 = 159984$, δηλαδή

$$A \leq 159984.$$

Από όλους τους αριθμούς μικρότερος ή ίσους του 159984 αυτός με το μεγαλύτερο άθροισμα ψηφίων είναι ο 99999, δηλαδή $B \leq 45$, και από όλους τους αριθμούς έως το 45 το μεγαλύτερο άθροισμα ψηφίων έχει ο 39.
Συνεπώς $\Gamma \leq 12$. Αλλά αποδείξαμε ότι $\Gamma \equiv 7(mod 9)$, άρα $\Gamma = 7$.

10. Όμοια με την § 2.6.1

11. Από το Θεώρημα Fermat έχουμε $\alpha^{p-1} \equiv 1(mod p)$ άρα

$$\alpha^p \equiv \alpha(mod p).$$

Από το Θεώρημα Wilson έχουμε $(p-1)! \equiv -1(mod p)$, άρα $(p-1)!\alpha \equiv -\alpha(mod p)$, οπότε $\alpha^p + (p-1)!\alpha \equiv 0(mod p)$.

12. Έστω

$$A = \binom{2p}{p} = \frac{(2p)!}{p!p!} = \frac{1\cdot 2\cdot 3\ldots(2p)}{(1\cdot 2\cdot 3\ldots p)^2}$$

$$= \frac{(p+1)(p+2)\ldots(2p-1)\cdot 2}{1\cdot 2\cdot 3\ldots(p-1)}$$

άρα

$$(1 \cdot 2 \cdot 3 \ldots (p-1))A = (p+1)(p+2)\ldots(2p-1) \cdot 2.$$

Θεωρώντας modulo$p$ και χρησιμοποιώντας το Θεώρημα Wilson, προκύπτει ότι:

$$(-1)A \equiv (-1) \cdot 2(mod p) \text{ ή}$$
$$A \equiv 2(mod p).$$

13. Για $p = 2$ έχουμε $2^p + 3^p = 13$, άρα $\nu = 1$.
Για $p > 2$ ο p πρέπει να είναι περιττός, άρα

$$2^p + 3^p \equiv 0(mod 5),$$

άρα $\alpha \equiv 0(mod 5)$.
Αν υποθέσουμε ότι $\nu > 1$ τότε $25 \mid \alpha^\nu$, άρα $25 \mid (2^p + 3^p)$.
Όμως

$$\frac{2^p + 3^p}{2+3} = 2^{p-1} - 2^{p-2} \cdot 3 + \ldots + 3^{p-1} \equiv p2^{p-1}(mod 5),$$

αδύνατο για $p \neq 5$.
Έτσι για $p \neq 5$ έχουμε $\nu = 1$.
Τέλος, για $p = 5$ ισχύει $2^p + 3^p = 753$, άρα πάλι προκύπτει ότι $\nu = 1$.

14. Αν $(\alpha, p) = (\beta, p) = 1$ τότε από το θεώρημα Fermat

$$\alpha^p \equiv \alpha(mod p) \text{ και } \beta^p \equiv \beta(mod p)$$

άρα η υπόθεση ισχύει αν και μόνο αν $\alpha \equiv \beta(mod p)$ οπότε η σχέση $\alpha^p \equiv \beta^p(mod p^2)$ είναι προφανής.
Αν $(\alpha, p) \neq 1$ τότε $\alpha \equiv 0(mod p)$ άρα και $\beta^p \equiv 0(mod p)$ ή $p \mid \beta^p$ ή $p \mid \beta$ ή $\beta \equiv 0(mod p)$ δηλαδή και εδώ $\alpha \equiv \beta(mod p)$ άρα $\alpha^p \equiv \beta^p(mod p^2)$. Όμοια αν $(\beta, p) \neq 1$.

Λύσεις Ασκήσεων § 3.1

1. Ο αριθμός 7 είναι πρώτος και από το Θεώρημα Fermat είναι φανερό ότι ο ακέραιος x ικανοποιεί τη σχέση $x^6 \equiv 1(mod 7)$ αν και μόνο αν ο x δεν είναι πολλαπλάσιο του 7.
Δηλαδή οι λύσεις της ισοτιμίας είναι οι 1,2,3,4,5,6 *modulo* 7.

2. Για το $mod 13$ έχουμε

$$\begin{aligned} 1^2 &\equiv 1(mod 13) \\ 2^2 &\equiv 4(mod 13) \\ 3^2 &\equiv 9(mod 13) \\ 4^2 &\equiv 3(mod 13) \\ 5^2 &\equiv 12(mod 13) \\ 6^2 &\equiv 10(mod 13). \end{aligned}$$

Από το Θεώρημα 3.2.2 υπάρχουν $(13-1)/2 = 6$ τετραγωνικά κατάλοιπα mod 13 κι αυτά είναι οι αριθμοί 1, 3, 4, 9, 10, 12.
Για το $mod 19$ έχουμε

$$\begin{aligned} 1^2 &\equiv 1(mod 19) \\ 2^2 &\equiv 4(mod 19) \\ 3^2 &\equiv 9(mod 19) \\ 4^2 &\equiv 16(mod 19) \\ 5^2 &\equiv 6(mod 19) \\ 6^2 &\equiv 17(mod 19) \\ 7^2 &\equiv 11(mod 19) \\ 8^2 &\equiv 7(mod 19) \\ 9^2 &\equiv 5(mod 19) \end{aligned}$$

και τα τετραγωνικά κατάλοιπα mod 19 είναι οι αριθμοί 1, 4, 5, 6, 7, 9, 11, 16, 17.
Για το $mod 31$, εργαζόμενοι όπως στα προηγούμενα, βρίσκουμε ότι τα τετραγωνικά κατάλοιπα mod 31 είναι 1, 2, 4, 5, 7, 8, 9, 10, 14, 16, 18, 19, 20, 25, 28. 28, 30, 33, 34, 36.

3. Ο αριθμός 7 διαιρεί τέλεια τον ν^2+2 αν και μόνο αν

$$\nu^2+2 \equiv 0(mod7) \text{ ή}$$
$$\nu^2 \equiv -2(mod7) \text{ ή}$$
$$\nu^2 \equiv 5(mod7)$$

το οποίο είναι άτοπο, διότι ο αριθμός 5 δεν είναι τετραγωνικό κατάλοιπο *mod* 7.

Λύσεις Ασκήσεων § 3.2

1. Έχουμε την ισοτιμία $x \equiv -3(mod p)$ η οποία έχει λύση αν και μόνο αν $\left(\frac{-3}{p}\right) = 1$.
   Επειδή $\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right)$ διακρίνουμε δύο περιπτώσεις:
   (i) Αν $p \equiv 1(mod 4)$, τότε $\left(\frac{-1}{p}\right) = 1$ και $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$
   (ii) Αν $p \equiv 3(mod 4)$, τότε $\left(\frac{-1}{p}\right) = -1$ και $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$

   Και στις δύο περιπτώσεις έχουμε ότι

$$\left(\frac{-3}{p}\right) = \left(\frac{p}{3}\right) = \left\{ \begin{array}{ll} \left(\frac{1}{3}\right) = 1 & , \alpha\nu \quad p \equiv 1(mod 3) \\ \left(\frac{2}{p}\right) = 1 & , \alpha\nu \quad p \equiv 2(mod 3) \end{array} \right\}$$

   Επομένως η ισοτιμία έχει λύση αν και μόνο αν $p \equiv 1(mod 3)$, δηλαδή όταν

$$p \equiv 1(mod 6) \ \ \acute{\eta}$$
$$p \equiv 4(mod 6).$$

   Όμως ο πρώτος αριθμός p είναι περιττός, άρα πρέπει να είναι της μορφής $p = 6\kappa + 1$.

2. Στο σύνολο $\Delta' = \{2, 3, \ldots, p-2\}$ όλοι οι αριθμοί μπορούν να χωρισθούν σε ζεύγη αντιστρόφων $mod p$, δηλαδή για κάθε αριθμό x υπάρχει μοναδικός αριθμός $y \neq x$, τέτοιος ώστε $x \cdot y \equiv (mod p)$. Επιπλέον, αν ο x είναι τετραγωνικό κατάλοιπο $mod p$, τότε το ίδιο είναι και ο y, αφού

$$1 = \left(\frac{1}{p}\right) = \left(\frac{xy}{p}\right) = \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = 1\left(\frac{y}{p}\right) = \left(\frac{y}{p}\right).$$

   Άρα το γινόμενο όλων των τετραγωνικών καταλοίπων $mod p$ στο διάστημα Δ' είναι $1(mod p)$.
   Ακόμη ο αριθμός 1 είναι πάντα τετραγωνικό κατάλοιπο, ενώ ο $p-1$ είναι τετραγωνικό κατάλοιπο $mod p$ αν και μόνο αν $p \equiv 1(mod 4)$.
   Άρα

$$A \equiv \left\{ \begin{array}{ll} 1 \cdot 1 \equiv 1(mod p) & , \alpha\nu \quad p \equiv 3(mod 4) \\ 1 - (p-1) \equiv -1(mod p) & , \alpha\nu \quad p \equiv 1(mod 4). \end{array} \right\}$$

3. Αν ο κ είναι σύνθετος και η κανονική του μορφή είναι

$$\kappa = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t},$$

τότε $\left(\frac{\kappa}{p}\right) = \left(\frac{p_1}{p}\right)^{\alpha_1} \left(\frac{p_2}{p}\right)^{\alpha_2} \dots \left(\frac{p_t}{p}\right)^{\alpha_t}$
Άρα, χωρίς τη βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι ο αριθμός κ είναι πρώτος.
Ακόμη, από τη σχέση $p = q + 4\kappa$ είναι φανερό ότι $p > \kappa$, $p \equiv q(mod4)$ και $p \equiv q(mod\kappa)$

i) Αν $\kappa \equiv 1(mod4)$, τότε

$$\left(\frac{\kappa}{p}\right) = \left(\frac{p}{\kappa}\right) = \left(\frac{q}{\kappa}\right) = \left(\frac{\kappa}{q}\right)$$

ii) Αν $\kappa \equiv 3(mod4)$, τότε

$$\left(\frac{\kappa}{p}\right) = \left(\frac{p}{\kappa}\right) = \left(\frac{q}{\kappa}\right) = \left(\frac{\kappa}{q}\right), \qquad \alpha\nu \quad p \equiv 1(mod4) \ \acute{\eta}$$

$$\left(\frac{\kappa}{p}\right) = -\left(\frac{p}{\kappa}\right) = -\left(\frac{q}{\kappa}\right) = \left(\frac{\kappa}{q}\right), \quad \alpha\nu \quad p \equiv -1(mod4)$$

Άρα, σε όλες τις περιπτώσεις ισχύει $\left(\frac{\kappa}{p}\right) = \left(\frac{\kappa}{q}\right)$.

Λύσεις Ασκήσεων § 3.3

1. Όμοια με την Εφαρμογή.

2. Όμοια με την Εφαρμογή.

Λύσεις Γενικών Ασκήσεων του 3ου Κεφαλαίου

1. Αν $p \geq 7$, τότε ένας τουλάχιστον από τους αριθμούς 2, 5, 10 θα είναι τετραγωνικό κατάλοιπο. Πράγματι, αν οι αριθμοί 2, 5 δεν είναι τετραγωνικά κατάλοιπα τότε $(\frac{10}{p}) = (\frac{2}{p})(\frac{5}{p}) = (-1)(-1) = +1$. Επίσης οι αριθμοί 1, 4, 9 είναι πάντα τετραγωνικά κατάλοιπα συνεπώς υπάρχουν δύο διαδοχικά τετραγωνικά κατάλοιπα.

2. Διακρίνουμε τις περιπτώσεις :

   - $\left(\frac{\nu^2+\varkappa}{p}\right) = 1$. Τότε μπορούμε να επιλέξουμε $x = \nu^2$ και $y = \nu^2 + \varkappa$.
   - $\left(\frac{(\nu+1)^2+\varkappa}{p}\right) = 1$. Τότε μπορούμε να επιλέξουμε $x = (\nu+1)^2$ και $y = (\nu+1)^2 + \varkappa$.
   - Εάν $\left(\frac{\nu^2+\varkappa}{p}\right) = -1$ και $\left(\frac{(\nu+1)^2+\varkappa}{p}\right) = -1$ τότε επιλέγουμε $x = (\nu^2+\nu+\varkappa)^2$ και $y = (\nu^2+\nu+\varkappa)^2 + \varkappa$, αφού $\left(\frac{(\nu^2+\nu+\varkappa)^2+\varkappa}{p}\right) = \left(\frac{(\nu^2+\varkappa)((\nu+1)^2+\varkappa)}{p}\right) = \left(\frac{\nu^2+\varkappa}{p}\right)\left(\frac{(\nu+1)^2+\varkappa)}{p}\right) = (-1)(-1) = 1$.

3. Θα αποδείξουμε ότι δεν υπάρχει αριθμός ν με τη ζητούμενη ιδιότητα.
   Έστω Σ το αρχικό σύνολο, Σ_1, Σ_2 τα δύο νέα σύνολα και Γ_1, Γ_2 τα αντίστοιχα γινόμενα. Εμείς θέλουμε $\Gamma_1 = \Gamma_2$ άρα θα έχουμε και $\Gamma_1 \equiv \Gamma_2 (mod 7)$.
   Θα αποδείξουμε ότι αυτό είναι αδύνατο. Κανένας από τους αριθμούς του Σ δε μπορεί να είναι πολλαπλάσιο του 7, αφού τότε η παραπάνω σχέση δεν θα ίσχυε, γιατί σε 6 διαδοχικούς αριθμούς ένας το πολύ θα είναι πολλαπλάσιο του 7. Έτσι οι αριθμοί του Σ είναι ισοϋπόλοιποι με 1,2,3,4,5 και 6 $mod 7$.
   Από το Θεώρημα Wilson το γινόμενο όλων των αριθμών είναι ισότιμο με $6! \equiv -1(mod 7)$, δηλαδή $\Gamma_1\Gamma_2 \equiv -1(mod 7)$ ή $\Gamma_1^2 \equiv -1(mod 7)$, αφού $\Gamma_1 = \Gamma_2$. Η παραπάνω σχέση είναι αδύνατη, αφού το (-1) δεν είναι τετραγωνικό κατάλοιπο $(mod 7)$.

Βιβλιογραφία

[1] Andrews, E. G. *Number Theory*. Saunders Company, Philadephia, 1971.

[2] Andrews, E. G. *Number Theory*. Dover, 1994.

[3] Apostol, T. M. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, 1976.

[4] Baker, A. *A Concise Introduction to the Theory of Numbers*. Cambridge University Press, 1984.

[5] Barbeau, E. J. *A Taste of Mathematics*. Canadian Mathematical Society, 1997.

[6] Bolker, D. E. *Elementary Number Theory: an analytic approach*. W.A. Benjamin Inc., New York, 1970.

[7] Burn, P. R. *A Pathway into Number Theory*. Cambridge University Press, 1982.

[8] Cassel, J. W. S. *"An Introduction to Diophantine Approximation."* Cambridge Tracts in Mathematics, 45, 1957.

[9] Cohen, H. *A Course in Computational Algebric Number Theory*. Spriger-Verlag, 1993.

[10] Cohn, H. *Advanced Number Theory*. Dover, 1962.

[11] Cox, A. D. *"Introduction to Fermat's Last Theorem."* American Mathematical Monthly 101, 1994, pp. 3–14.

[12] Davenport, H. *Multiplicative Number Theory.* Springer-Verlag, 1980.

[13] Davenport, H. *The Higher Arithmetic.* Cambridge University Press, 6th edition, 1992.

[14] Davenport, H. *The Higher Arithmetic.* Cambridge University Press, 1992.

[15] Dudley, U. *Elementary Number Theory.* Freeman, 2nd edition, 1978.

[16] Ellison, W. and Ellison, F. *Prime Numbers.* Wiley, 1985.

[17] Estermann, T. *"Introduction to Modern Prime Number Theory."* Cambridge Tracts in Mathematics, 42, 1952.

[18] Gouvêa, F. *"A Wonderful Proof."* American Mathematical Monthly 101, 1994, pp. 203–222.

[19] Graham, R., Knuth D. and Patashnik O. *Concrete Mathematics.*, 2nd Edition.

[20] Greitzer, S. L. *International Mathematical Olympiads, 1959–1977.* MAA, 1978.

[21] Gupta, H. *Selected Topics in Number Theory.* Abacus Press, 1980.

[22] Guy, K. P. *Unsolved Problems in Number Theory, volume 1.* Springer-Verlag, 1981.

[23] Haberstain, H. and Richert, H.E. *Sieve Methods.* Academic Press, 1974.

[24] Hall, M. I. *Topics in Number Theory.* University of Keele, 1984.

[25] Honsberger, R. *Mathematical gems II.* Mathematical Association of America, 1973.

[26] Karatsuba, A. A. *Basic Analytic Number Theory.* Springer-Verlag, 1993.

[27] Klamkin, M. S. *USA Mathematical Olympiads, 1972–1986.* MAA, 1988.

[28] Koblitz, N. *A Course in Number Theory and Cryptography.* Springer-Verlag, 1987.

[29] Leveque, J. W. *Fundamentals of Number Theory.* Addison-Wesley, 1977.

[30] Mitrinović, S. D., Sándor J. and Crstici B. *Handbook of Number Theory.* Kluwer Academic, 1996.

[31] Niven, I. and Zuckerman, S. H. *An Introduction to the Theory of Numbers.* Wiley Eastern, 3rd edition, 1972.

[32] Niven, I., Zuckerman, S. H. and Montgomery L. H. *An Introduction to the Theory of Numbers.* Wiley Eastern, 5th edition, 1991.

[33] Ore, O. *Invitation to Number Theory.* Mathematical Association of America, 1967.

[34] Parent, D. P. *Exercises in Number Theory.* Springer-Verlag, 1984.

[35] Parshin, N. A. and Shafarevich R. I. *Number Theory I: fundamental problems, ideas and theories (Teoriīa chisel 1).* Springer, 1995.

[36] Redmond, D. *Number Theory: an introduction.* Marcel Dekker Inc., 1996.

[37] Riesel, H. *Prime Numbers and Computer Methods for Factorisation.* Birkhauser, 1985.

[38] Rose, E. H. *A Course in Number Theory.* Clarendon Press, Oxford, 1988.

[39] Rosen, N. K. *Elementary Number Theory and its Applications.* Addison-Wesley, (AT&T Bell Laboratories), 2nd edition, 1988.

[40] Schumer, D. P. *Introduction to Number Theory.* International Thomson Publishing, 1996.

[41] Stark, M. H. *An Introdction to Number Theory.* Markham Publishing, Chicago, 1971.

[42] Vaughan, R. C. *"The Hardy-Littlewood Method."* Cambridge Tracts in Mathematics, 80, 1981.

[43] Weiss, E. *First Course in Algebra and Number Theory.* Academic Press, New York, 1971.

[44] Βλάμος, Π. Μ. *"Μία Στοιχειώδης Απόδειξη του Θεωρήματος Lagrange."* Μαθηματική Επιθεώρηση 49, 1998.

[45] Βλάμος, Π. Μ. *"Πρόταση Θεμάτων σε Διεθνείς Μαθηματικές Ολυμπιάδες-Προετοιμασία Ολυμπιακών Ομάδων."* Μαθηματική Επιθεώρηση 50, 1998.

[46] Βλάμος, Π. Μ. *"Η Δομή της Θεωρίας των Αριθμών."* Ερευνητικό Κέντρο Αξιολόγησης και Επιμόρφωσης της Ε.Μ.Ε., 1999.

[47] Βλάμου Ε., Βλάμος Π., Οικονόμου Α., Ράππος Ε. και Ψαρράκος Π. *"Διαμερίσεις Ακεραίων στις Διεθνείς Μαθηματικές Ολυμπιάδες."* Μαθηματική Επιθεώρηση 51, 1999.

Ευρετήριο Όρων

αθροισμα διαιρετών, 64
αλγόριθμος της διαίρεσης, 2
αλγόριθμος του Ευκλείδη, 22
ανηγμένο σύστημα υπολοίπων, 96
αντίστροφος ως προς mod ν, 79

γραμμική διοφαντική εξίσωση, 36

διαιρετέος, 2
διαιρετότητα, 12
διαιρέτης, 2
δίδυμοι πρώτοι, 55

ελάχιστο κοινό πολλαπλάσιο, 45
ευκλείδεια διαίρεση, 1

ημέρα της εβδομάδας, 114

θεώρημα
    Euler, 105
    Fermat, 105
    Fermat, μεγάλο, 180
    Lucas, 106
    Wilson, 111
    θεμελιώδες αριθμητικής, 52
    κινέζικο υπολοίπων, 90
    πρώτων αριθμών, 154

ισοϋπόλοιποι, 2, 77

κανονική μορφή, 53
    Ε.Κ.Π., 53
    Μ.Κ.Δ., 53
κριτήρια διαιρετότητας, 12, 113
κριτήριο Euler, 125
κριτήριο ρίζας, 51
κρυπτοσύστημα RSA, 174
κόσκινο του Ερατοσθένη, 164

λήμμα του Gauss, 128
λήμμα του Ευκλείδη, 27

μη-τετραγωνικά κατάλοιπα, 124
μέγιστος κοινός διαιρέτης, 22
μέθοδος Hardy-Littlewood, 158

νόμος τετραγωνικής αντιστροφής, 133

παράγοντας, 12
πηλίκο, 1
πλήθος διαιρετών, 64
πολλαπλάσιο, 12, 18
πρόβλημα Goldbach, 161
πρόβλημα Waring, 162
πρώτοι μεταξύ τους αριθμοί, 22
πρώτος, 51

συνάρτηση Euler, 65, 96
σχετικά πρώτοι αριθμοί, 22
σύμβολο του Legendre, 131
σύνθετος, 51

σύστημα γραμμικών ισοτιμιών, 90

τετραγωνικά κατάλοιπα, 124
τετριμμένοι παράγοντες, 12
τέλειος αριθμός, 66

υπόλοιπο, 1

ψηφία
    περιττής τάξης, 13
    άρτιας τάξης, 13